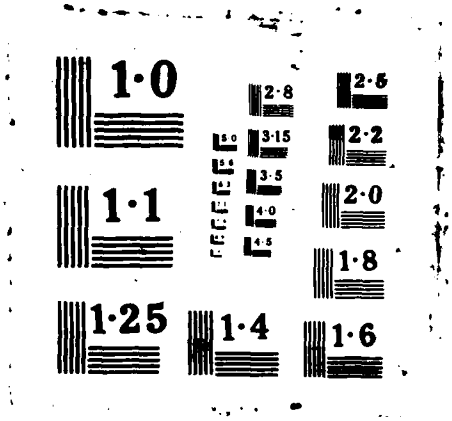
AD-A177 932   SECURE VOICE SYSTEM INTEGRATED CONFERENCING ANALYSIS   1/2
AND INTEROPERATION DESIGN(U) COMPUTER SCIENCES CORP
FALLS CHURCH VA SYSTEMS DIV G KNOWLES ET AL. 17 FEB 87
UNCLASSIFIED   DCA100-84-C-0030   F/G 17/2   NL


1·0
2·8
2·5
3·15
2·2
3·5
2·0
4·0
1·1
4·5
1·8
1·25
1·4
1·6

DEFENSE COMMUNICATIONS ENGINEERING CENTER

SECURE VOICE SYSTEM INTEGRATED CONFERENCING ANALYSIS AND INTEROPERATION DESIGN

13 FEBRUARY 1987

DEFENSE COMMUNICATIONS ENGINEERING CENTER

SECURE VOICE SYSTEM
INTEGRATED CONFERENCING ANALYSIS
AND
INTEROPERATION DESIGN

13 FEBRUARY 1987

Prepared by
COMPUTER SCIENCES CORPORATION
Under
CONTRACT DCA100-84-C-0030

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

1b. RESTRICTIVE MARKINGS
None

2a. SECURITY CLASSIFICATION AUTHORITY
[redacted]

2b. DECLASSIFICATION/DOWNGRADING SCHEDULE
[redacted]

3. DISTRIBUTION/AVAILABILITY OF REPORT
Unlimited

4. PERFORMING ORGANIZATION REPORT NUMBER(S)

5. MONITORING ORGANIZATION REPORT NUMBER(S)

6a. NAME OF PERFORMING ORGANIZATION
Computer Sciences Corporation
Systems Division

6b. OFFICE SYMBOL *(If applicable)*
354

7a. NAME OF MONITORING ORGANIZATION

6c. ADDRESS *(City, State and ZIP Code)*
3160 S. Fairview Park Drive
Falls Church, VA 22042

7b. ADDRESS *(City, State and ZIP Code)*

8a. NAME OF FUNDING/SPONSORING ORGANIZATION
Defense Communications
Engineering Center

8b. OFFICE SYMBOL *(If applicable)*
B230

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
DCA100-84-C-0030

8c. ADDRESS *(City, State and ZIP Code)*
1860 Wiehle Avenue
Reston, VA 22090

10. SOURCE OF FUNDING NOS.

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT NO.

11. TITLE *(Include Security Classification)* Secure Voice System Integrated Conferencing Analysis and Inter-Operation Design - UNCLASSIFIED

12. PERSONAL AUTHOR(S)
Knowles, G.; Bernet, M.; Doyle, S.

13a. TYPE OF REPORT
FINAL

13b. TIME COVERED
FROM 3/86 TO 2/87

14. DATE OF REPORT *(Yr., Mo., Day)*
1987 FEB 17

15. PAGE COUNT

16. SUPPLEMENTARY NOTATION

17. COSATI CODES

FIELD	GROUP	SUB. GR.

18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
Secure Conferencing Project, RED Switch Project, General Purpose Conferencing, STU-III, SVS Interoperability, SVS Numbering Plans, Conference Setup Procedures

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

This report establishes functional requirement guidelines for those agencies tasked to design the Secure Voice System (SVS). The SVS is comprised of the Secure Conferencing Project (SCP), the RED Switch Project, and General Purpose Conferencing. For each of the aforementioned subsystems, a numbering plan was developed, a list of data tables was defined, and conference setup procedures were outlined. An analysis of the interoperation of the three subsystems was done and any issues or problems ahve been defined and a recommended solution provided.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT
UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. □ DTIC USERS □

21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL
Robert Donald

22b. TELEPHONE NUMBER *(Include Area Code)*
202/437-2150

22c. OFFICE SYMBOL
R630

EDITION OF 1 JAN 73 IS OBSOLETE.

TABLE OF CONTENTS

Page

TABLE OF CONTENTS (Cont.)

TABLE OF CONTENTS (Cont.)

RE: Classified References, Distribution Unlimited
No change in the distribution statement
Per Mr. Robert Donald, DCEC/R630

LIST OF ILLUSTRATIONS

EXECUTIVE SUMMARY

Secure voice and conferencing requirements for DoD will be satisfied by several initiatives that will comprise the Secure Voice System (SVS). The SVS architecture consolidates the capabilities of the NSA Future Secure Voice System (FSVS), the RED Switch Project, the Secure Conferencing Project (SCP), and General Purpose (GP) Confernciing (which is expected to be separated from the SCP project in the near future and become a capability provided by AUTOVON/DSN). The SCP will provide conferencing for Command and Control (C^2) users. General Purpose Conferencing will provide conferencing for Type I STU-IIIs in AUTOVON/DSN and will be dealt with separately from SCP in this report. The RED Switch Network supports C^2 secure voice users who are located within a physically secured enclave (RED enclave). These RED Switches will be networked together by direct encrypted interswitch trunks.

The SVS will provide user-friendly, automatic, and interoperable secure voice service to support the C^2 missions of the National Command Authorities (NCA) and selected supporting elements. The SVS will also provide user-friendly secure voice service to satisfy general purpose missions of the DoD as resources permit. Non-DoD entities may obtain SVS service in order to satisfy special defense-related requirements, when approved by the Assistance Secretary of Defense (C^3I) in coordination with the Joint Chiefs of Staff.

The specification for the RED Switch [2] and the SVS Goal Architecture [6] both state that the three subsystems (GP, SCP C^2, and RED Switch) will interoperate. The objective of this task is to provide the DCA with a design showing how the SVS subsystem should interoperate efficiently. This report will provide functional requirement guidelines for those agencies tasked to develop the SVS.

The Numbering Plan, Data Tables, Data Transfer, Conference Set-up Procedures, and Analysis provided in this report describe a potential architecture for the interoperation of the three major secure conferencing systems. The Numbering Plan developed in this report is consistent with the DSN Worldwide Numbering Plan. The Numbering Plan was designed to be convenient to use, and be compatible with existing local and extended dialing formats wherever possible. The Data Tables define what data must be maintained in each of the SVS components and what function each data element serves in order to permit authorized users to establish preset or random conferences. The Data Transfer and Conference Set-Up Procedures define the sequence of events required for the different SVS components to interoperate. However, certain issues, concerns, and problems were encountered whole developing and analyzing these architectures. Several possible solutions to these problems are provided along with our recommendations. Some issues are still unresolved and some solutions may be imperfect due to various constraints. These crucial issues (related to conferencing subsystem interoperation) are highlighted in the following paragraphs.

ISSUES

The GP Conference Director will support all security levels through TOP SECRET. However, limitations in the RED Interface Terminal (RIT) (note: the RIT is a STU-III which can be interfaced to other hardware such as a Conference Director) restrict the manner in which a connection is achieved.

When initiating a conference, the security level of each conferee must be set to the same level as the conference originator or at the level requested by the conference originator (the CD will not allow the conference originator to surpass their authorized security level). Presently, the RIT cannot be set to more than one security level at a time. This prevents a Conference Director from controlling the security level at which a conferee is called. Thus a conferee's STU-III display may read SECRET when the conference originator's security level is only CONFIDENTIAL. The RIT should ideally be modified to allow the security level to be set remotely. At present this does not seem to be an option in the STU-III/RIT design. Barring this solution, two other viable solutions remain. The first method is to segregate the Conference Directors so that a certian set of Conference Directors serves TOP SECRET users, another set serves SECRET users, and a third set that serves CONFIDENTIAL users. This alternative may not use AUTOVON/DSN resources efficiently since a Conference Director with the appropriate security level for a given call may not be the closest Conference Director to the caller. Also, the mix of Conference Directors operating at the three security levels can not be changed in real-time, which could become a problem if a certain security level Conference Director becomes saturated while the other security level Conference Directors still have plenty of room. The second (and recommended) alternative is to put three RITs at each of the Conference Directors' ports and have the Conference Director select the RIT with the desired security level. This alternative will triple the number of required RITs but will allow greater versatility and use AUTOVON/DSN resources more efficiently.

Another deficiency of the RIT is its inability to automatically force a distant STU-III to enter the secure mode. Presently, the only solution to this problem is for the Conference Director to continuously instruct the RIT to go secure until the RIT acknowledges a secure connection or the Conference Director's time-out period has expired.

There are now over a million STU-III's projected that may have access to the GP Conference Directors. If all of these users are allowed to originate a conference, a method must be developed so that the Conference Director can ascertain certain information about the user's authority for conferenc origination. The original plan was to store this data in the memory of the

Conference Director. In fact, this would be the preferred way if the number of STU-IIIs was relatively small. However, now with over a million users, it would be very man-power intensive to maintain and update all this information in the memory of the Conference Directors. We recommend that this information be included in the STU-III ID Field along with the Terminal ID and Security Level of the STU-III. This information could then be passed from the STU-III to the RIT and finally to the Conference Director. NSA would have to agree to allocate the ID Field space and be responsible for programming this additional information into a unique terminal ID field.

We also recommend that the user's name not be included in the STU-III ID Field since this would seriously impact data management. Since more than one person may be using or have access to a particular STU-III, associating a name with a terminal has little meaning. From a data management standpoint, personnel changes are made relatively frequently and department mission and requirements are relatively static. Every time there is a personnel change, the ID would have to be updated, but if a department moved locations, the STU-III could simply be taken to the new location without interrupting service.

Similarly, an analogous situation exists with the SCP C^2 Conference Director. There will be a few situations where the conference originator will be entering the SCP Conference Director through AUTOVON/DSN. First, a few remote SCP C^2 users exist who can only access the SCP C^2 Conference Director via a STU-III and AUTOVON/DSN. Second, some SCP C^2 users may have to access another SCP C^2 via their SCP Conference Director and an RIT in a backup mode. Since there are less than one hundred SCP C^2 users (and data management is not the problem as it is in GP conferencing), we recommend that the conference authorization be performed by verification of the STU-III Terminal ID against a look-up table in the SCP Conference Director.

The manner in which SCP C^2 and the RED Switch interoperate is of great concern. The SCP Conference Director is self-authenticating to the TOP SECRET level and the RED Switch is self-authenticating to the SECRET level, and both systems allow for verbal authentication up to the TS/SCI level. Only a RED Switch user with a TOP SECRET classmark can be classmarked to call the SCP C^2 Conference Director. However, the lack of trusted software (software security as described in the Orange Book) in the RED Switch will not permit automatic self authentication of such calls higher than SECRET. Even users within a RED Switch SCIF would have to verbally authenticate each telephone call, even to other people within the SCIF. If the software in the RED Switch is not trusted, someone could easily reassign the line number of someone within the SCIF to a phone outside the SCIF. For this reason, all connections between the SCP C^2 Conference Director and the RED Switch will initially be SECRET, and an announcement will be provided as a reminder at conference start stating that their are SECRET conferees connected to the conference. Similarly, if a SECRET user from the GP is included in a SCP C^2 conference, an announcement is also made. It will be left up to the conferees to verbally authenticate up to as high as TS/SCI. The only alternative to this is to have some form of physical security. For example, the users in a RED Switch SCIF could verbally authenticate their calls within the RED Switch and use separate phones that are physically secured and directly connected to the SCP Conference Director.

Almost all of the developed designs involving SCP in this report went under the assumption that SCP FOC will be as described in the SCP A Specification. Recently, the question has been raised whether or not this is true. Currently, the major concern is whether or not the SCP C^2 EOC equipment/software and procedures will be incorporated into the SCP C^2 FOC design. Certain deficiencies and incompatibilities in EOC (such as a slower call establishment time and different COMSEC) may cause problems transitioning from EOC to FOC. A successful phase-in from EOC to FOC operation will depend on the degree to which FOC is compatible with the EOC system.

There is presently no method of transferring a RED Switch user's classmark to AUTOVON/DSN. The RED Switch provides no screening for these lines. Thus, all RED Switch users will have the same classmark in AUTOVON/DSN and the same privileges at the GP Conference Director. This means that most RED Switch users will have a different classmark in AUTOVON/DSN than they have within the RED Switch.

When conferencing in GP, there are three methods in which conferees can be brought into a large conference. First, they could all be brought in directly to a single Conference Director. This method does not use AUTOVON/DSN resources efficiently. Second, two or more conferees could be brought in by their local Conference Director and then be bridged to the originating Conference Director. This method may not use GP conferencing resources efficiently. The third (and recommended) method is to use a topological design algorithm to dynamically calculate the most efficient manner in which a conference is to be configured. The Conference Director using this algorithm will determine in real-time the optimal or near-optimal configuration for the conference upon completion of dialing data from the conference originator. This method uses both AUTOVON/DSN and conferencing facilities relatively efficiently.

As expected, the majority of the interoperation problems were security related. The major stumbling blocks were the limitations of the RIT and differences in security levels of the SVS components.

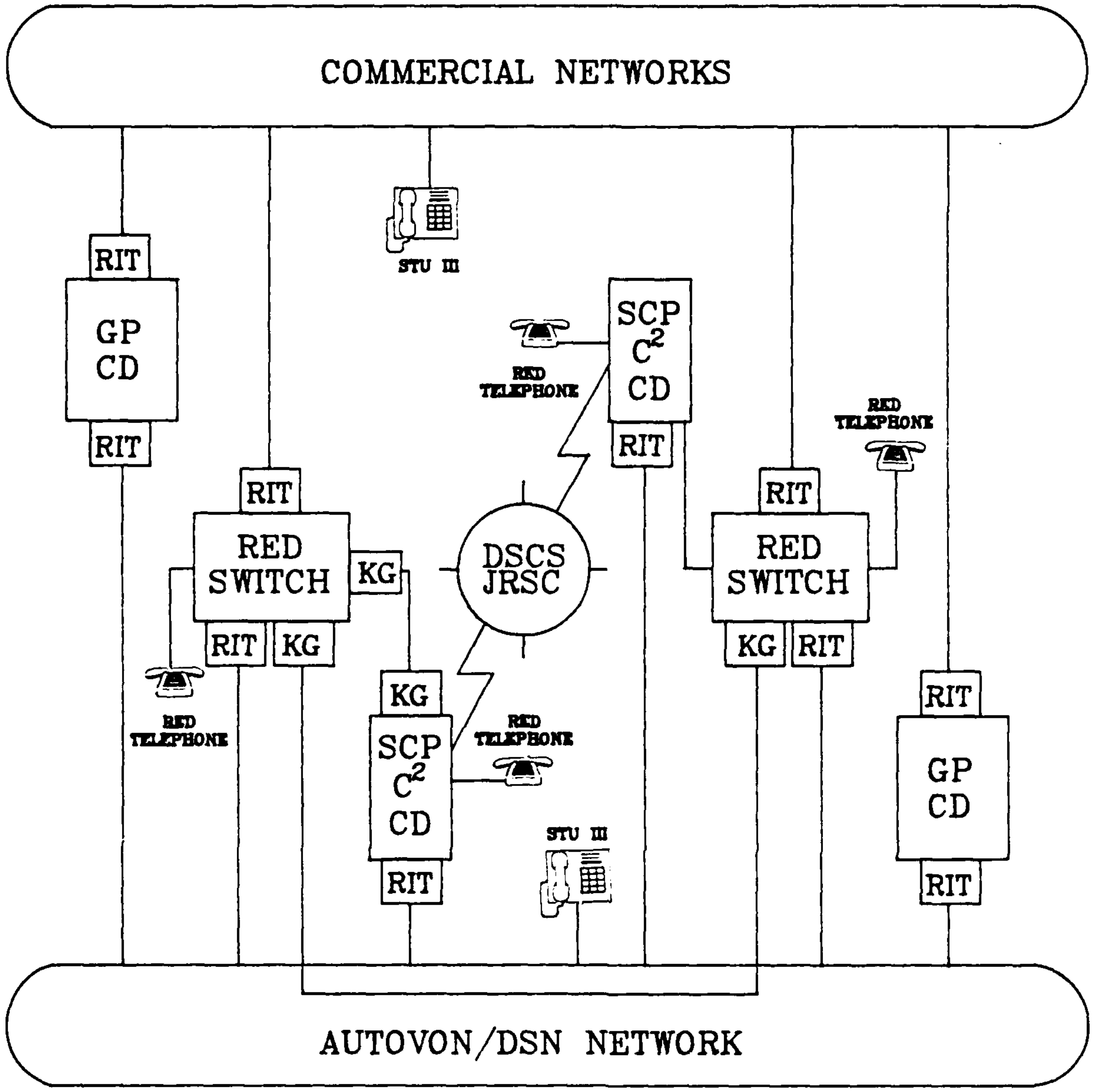
SECTION 1 - INTRODUCTION

Secure voice and conferencing requirements for the DoD will be satisfied by several initiatives that will comprise the Secure Voice System (SVS). The SVS architecture consolidates the capabilities of the NSA Future Secure Voice System (FSVS) Program, the Secure Conferencing Project (SCP), the General Purpose (GP) Conferencing Project, and the RED Switch Project. The STU-III family of equipment being developed as part of the FSVS program will be the primary secure voice terminal used within the SVS. The SCP will provide conferencing for Command and Control (C^2) users. GP conferencing is being dealt with separately from the SCP. The RED Switch will function as a Private Branch Exchange (PBX) for unencrypted secure voice traffic and will contain necessary features to satisfy C^2 requirements. Encrypted interfaces will connect RED Switches to components of the SVS that are not collocated. A generic line diagram of the SVS is contained in Illustration 1-1. Although commercial connectivity is shown, it will not be addressed in any detail in this report.

The SVS will provide user-friendly, automatic, and interoperable secure voice service to support the C^2 missions of the National Command Authorities (NCA) and selected supporting elements under peacetime, crisis/pre-attack and early transattack conditions. The SVS will also provide user-friendly secure voice service to satisfy general purpose missions of the DoD in peacetime and under stressed conditions, as resources permit. Non-DoD entities may obtain SVS service in order to satisfy special defense-related requirements, when approved by the Assistant Secretary of Defense (C^3I) in coordination with the Joint Chiefs of Staff (JCS).

1.1 PURPOSE

The specifications for the RED Switch and the SVS goal architecture both state that the three subsystems (GP, SCP C^2, and RED Switch) will interoperate with each other. The objective



CD	–	CONFERENCE DIRECTOR
DSCS	–	DEFENSE SATELLITE COMMUNICATION SYSTEM
GP	–	GENERAL PURPOSE
JRSC	–	JAM RESISTANT SECURE COMMUNICATION
KG	–	KEY GENERATOR
RIT	–	RED INTERFACE TERMINAL
SCP	–	SECURE CONFERENCE PROJECT

Illustration 1-1. Generic Line Diagram of SVS

of this task is to provide the DCA with a design of how the SVS subsystems should efficiently interoperate; and also establish baseline requirements for the agency tasked to design the SVS.

1.2 SCOPE

This report culminates the efforts of all previous draft reports prepared under this task. It will discuss the interoperation of the SVS network shown in Illustration 1-1 with the exception of the commercial networks.

For each of the three conferencing subsystems described in this report, a Numbering Plan has been developed to be compatible with the DSN Worldwide Numbering Plan. A set of Data Tables and the necessary data transfer required for conferencing has been identified. Conference Setup Procedures and an analysis of SVS interoperation have been discussed in detail for the connectivity shown in Illustration 1-2. Along the way, certain problems were uncovered. In these cases, potential solutions have been offered along with our recommendation. Where problems could not be solved, assumptions were made to work them out.

	SUBSCRIBER CONNECTION						SECONDARY BRIDGE CONNECTION			
	STU-III		RS SUB		SCP C^2 SUB		SCP C^2	GP	RS ANALOG	RS DIGITAL
	O	P	O	P	O	P	CD	CD	CB	CB
SCP C^2 CD	(1)	X	(1)	X	X	X	X	-	(6)	-
GPCD	X	X	(4)	(2)	-	-	-	X	(2) (4)	-
RS ANALOG CB	(2)	(5)	X	X	-	-	(6)	(2)	(3)	-
RS DIGITAL CB	(2)	X	X	X	-	-	-	-	-	-

NOTE: Read Illustration Top to Bottom and then Right to Left.

Legend:

X	=	Capability
-	=	No Capability
P	=	Participant
O	=	Originator
CB	=	Conference Bridge
GP	=	General Purpose
RS	=	RED Switch
SCP	=	Secure Conference Project

Notes:

(1) If Authorized

(2) RS Attendant Only

(3) Preset-Auto Via Dedicated RS Trunks
Random-Attendant setup

(4) Limited To Capabilities of RS
Interface Terminal, i.e., No Screening in RS.

(5) Limited To One STU-III, If No RS Digital CB

(6) Only When Collocated or Directly Connected
Through KG Units

Illustration 1-2. Secure Conference Connectivity

SECTION 2 - SECURE VOICE SYSTEM (SVS) ARCHITECTURE OVERVIEW

2.1 SVS SUBSYSTEMS

The Secure Voice System is comprised of General Purpose (GP), Secure Conference Project (SCP) C^2 and RED Switch subsystems. These subsystems are interconnected using existing and evolving DCS voice grade communications networks. Interoperability is achieved wherever possible by providing automatic interfaces between those equipment which cannot be made directly interoperable with each other. The SVS supports Multilevel Precedence and Preemption (MLPP), and each subscriber will be classmarked to indicate calling privileges or restrictions.

2.1.1 General Purpose STU-III Conferencing Subsystem

The GP conferencing subsystem supports secure voice conferencing requirements of DoD STU-III subscribers worldwide. This subsystem consists primarily of the STU-III and its associated RED Interface Terminal (RIT) which use the FIREFLY system. The STU-III and the RIT appear as alternate voice/data subscribers to the AUTOVON/DSN and commercial networks. A public key system is used to provide the STU-III's secure communication.

2.1.2 SCP C^2 Subsystem

The SCP C^2 subsystem supports the unique requirements of critical C^2 users. This subsystem must be highly reliable and highly survivable. It provides secure voice and secure graphics preset and random conferencing service to critical C^2 users, designated remote C^2 users, NEACP commanders, and authorized afloat commanders. Interconnection among the SCP C^2 Conference Directors (CDs) worldwide is accomplished via the Jam Resistant Secure Communications System (JRSC) which will provide survivability during trans-attack periods. For redundance and interoperability with other components of the SVS, the CD's will also be interconnected through RIT interfaces to the AUTOVON/DSN, and directly to collocated RED Switches.

2.1.3 RED Switch Subsystem

The RED Switch subsystem supports C^2 secure voice users that are located within a physically securable enclave (RED enclave). Each RED Switch forms a switching hub for its own RED enclave. Users within the RED enclave will have telephone sets connected to the RED Switch by physically secured unencrypted loop circuits for high quality voice communications. RED Switches will be netted together by encrypted RED Switch interswitch trunks. Some RED Switches will also have DSVT links to the TRI-TAC subsystem, and trunks to collocated SCP C^2 CD's. RED Switches will also interoperate with STU-IIIs and KY-77s via RIT interfaces to AUTOVON/DSN and commercial telephone networks.

2.2 SVS COMPONENTS

The major SVS components as shown in Illustration 1-1 include user terminals, interface devices and conferencing nodes.

2.2.1 RED Telephones (RED phones)

RED telephones are operationally equivalent to standard clear telephone sets, but are certified to meet NSA and DIA standards for processing classified conversations. RED telephones will normally be employed to support users located in an enclave served by a RED Switch, and will serve as the telephone instrument for the SCP CD. Connection to the SVS for RED phones behind a RED Switch will be via RED subscriber loops to the serving RED Switch. Encrypted RED Switch interfaces will extend the connection to other components of the SVS via the AUTOVON/DSN, commercial networks, and direct inter RED Switch trunks. The traffic between RED telephones connected to the same RED Switch will not require encryption as long as the entire cable plant is protected in a secure environment.

2.2.2 STU-III Family

The STU-III (Secure Telephone Unit, Third Generation) family of self contained secure telephone sets provide full-duplex speech security via standard two-wire access to government and commercial telephone networks. The STU-IIIs employ an enhanced 2400 bps Linear Predictive Coding algorithm (LPC-10E). Two categories of STU-IIIs will be available. Type I STU-IIIs will be approved for securing all levels of classified traffic and will be available in at lest three commercial versions plus the full government specified KY-77. Type II STU-IIIs will provide security for sensitive unclassified traffic, primarily in non-government applications. For more information on the STU-III see Appendix A.

2.2.3 STU-III RED Interface Terminal (RIT)

The RIT is a variant of the STU-III which provides RED analog, RED digital, control, and status input/outputs to interface STU-IIIs to other components of the SVS. The secure voice interface will be digital to preserve voice quality whenever the interfaced component employs a compatible LPC-10 algorithm. The RIT also provides for the receipt of secure dialing data from STU-III users when required to control automatic interfaces. Specifically the RIT will be used to interface STU-IIIs to at least the following:

1. SCP C^2 CD via AUTOVON/DSN
2. GP Conference Bridge
3. RED Switch via AUTOVON/DSN and commercial networks.

The RIT will be required to pass certain information to the CD it is connected to and receive certain information from the CD. It will have the ability to pass at least the following information to the Conference Director:

1. The identification of the calling terminal
2. The classification level of a connection established with a STU-III to the CD.

In all cases, the RIT will operate automatically (i.e., no manual intervention). When a terminal places a call to a CD, the

AUTOVON/DSN will provide a connection to the RIT connected to the CD. The RIT and the STU-III will automatically go into the secure mode, in which the connection will be established to the highest mutual classification level. ID Field information would also be exchanged, which would identify the calling terminal. Once synchronization is achieved with the RIT, the user is connected to the conference director in the secure mode. The user can then give detail dialing instructions to the CD regarding whom he wishes to include in a conference.

2.2.4 Key Generator (KG)

The KGs used in the SVS are full-duplex, digital encryption devices used for securing digital trunks. The KG-84A would be used to secure single channel trunks like those between connected RED Switches and a noncollocated SCP C^2 CD. KG-81's would be used to encrypt trunk groups.

2.2.5 General Purpose Conference Director

The General Purpose Conference Director (CD) will provide preset or random noninterruptible speaker controlled voice conferencing between General Purpose STU-III users. Conferencing will be accomplished digitally without analog conversion to preclude degradation of voice quality. The CD will be connected through RIT's to STU-III subscribers.

2.2.6 SCP C^2 Conference Director

The SCP C^2 Conference Director (CD) is a fast digital switch that will provide preset or random noninterruptible speaker controlled voice and/or graphics conferencing between designated C^2 users. Interfaces will automatically adjust to the lowest conferee's transmission rate. Conferencing will be accomplished digitally without analog conversion to preclude degradation of voice quality. The SCP C^2 CD will provide dynamic controls necessary for operation over DSCS/JRSC satellite systems and will be capable of bridged conferencing with local and remote users of other SCP C^2 CD's worldwide. SCP C^2 conferencing will be extendable to other SVS users as required. The SCP C^2 CD will include COMSEC equipment to provide key variables on a per call/conference basis for the DSCS/JRSC derived links between conference nodes. The SCP C^2 CD's will be interconnected via the JRSC, connected to the SVS via STU-III RED Interface Terminals (RIT's), and directly connected to collocated RED Switches. The SCP C^2 CD will include an attendant console to provide conference assistance although most conferences will be established through direct dialing by the conference originator.

2.2.7 RED Switches

The RED Switch is a secure digital PBX that will serve C^2 SVS users within a securable area (RED enclave). It will allow users to exchange secure voice communications from clear telephone sets certified for sensitive and classified communications. Calls to or from the SVS outside the RED enclave will be accommodated via encrypted interfaces to the AUTOVON/DSN, commercial networks and TRI-TAC. Encrypted ditital trunks will be provided between RED Switches to provide a cost effective, high quality RED Switch network. Designated RED Switches will also be directly connected to a collocated SCP CD. The RED Switch will include an attendant console for local and bridged call assistance and will provide modern automatic PBX features. A preset and random conferencing capability will be inherent in the RED Switch. RED Switches will be modular and capable of accommodating requirements of between 100 and 1500 lines.

2.3 AUTOVON/DSN

The global Automatic Voice Network (AUTOVON) is the principal long-haul, common-user, switched voice communications network for DoD agencies concerned with matters of national defense. It provides worldwide, direct distance dialing through a system of Government-owned and leased automatic switching and transmission facilities.

Although AUTOVON is not being developed as part of the SVS, its resources will be used. The primary mission of AUTOVON is to provide rapid, worldwide, Command and Control (C^2) voice communications to the National Command Authority (NCA) and other high-priority users. Its secondary mission is to provide telephone service for operational, intelligence, logistic, administrative, and diplomatic use. AUTOVON serves two categories of users: four-wire subscribers who require immediate access to the network and whose telephones are directly connected to an AUTOVON switch, and two-wire subscribers who gain access to the network through local PBXs by dialing an access code or through a local PBX operator. The AUTOVON system also has a Multilevel Precedence Preemption (MLPP) feature that gives calling priority to authorized users (see Appendix B). Users are assigned a calling precedence based on operational mission requirements.

The DSN will evolve from the existing AUTOVON network and will provide endurable, rapid, and economical telecommunications for high priority users, as well as service to lower priority users on a non-interference basis with high priority users.

The worldwide DSN will consist of three subnetworks: WESTHEM, Pacific, and Europe. The WESTHEM DSN is currently still under design. The Pacific DSN will consist of approximately 18 backbone switches, richly connected primarily through satellite connectivity. The Europe DSN will consist of approximately 46 backbone switching nodes, richly connected primarily through terrestrial connectivity.

AUTOVON funding is presently based on the capability that is provided concerning maximum calling area and precedence. The cost for a 4-wire access line is not based on a charge for service used but on the capability provided. The user community, DCA, and OSD, are currently studying the feasibility of charging customers on the number of calls actually placed by users. This would provide the users with more billing information and as a result, provide them with more direct control over the costs.

In the SVS, the General Purpose (GP) STU-III's network will use AUTOVON/DSN. SCP C^2 will use AUTOVON/DSN as a backup network and also for calling GP users. The RED Switch network will be connected through dedicated AUTOVON/DSN trunks.

SECTION 3 - GENERAL PURPOSE STU-III CONFERENCING

3.1 INTRODUCTION

The General Purpose (GP) secure conferencing subsystem will provide the GP community of users with a secure voice capability. It will be comprised of secure Conference Directors (CDs), STU-III telephone terminals, RED Interface Terminals (RITs), a public key system, and the transmission resources of AUTOVON/DSN.

In the past GP conferencing has been part of the Secure Conference Project (SCP) but it is anticipated that GP will be separated from SCP and became a capability provided by DSN in the future. The STU-III family of equipment being developed as part of the Future Secure Voice System (FSVS) program will be the primary secure voice terminals used for GP conferencing. Primary connectivity between the voice terminals and conference bridges will be provided by AUTOVON/DSN. An essential element of conferencing is a numbering system that is compatible with existing systems, readily understandable, and convenient to use. This section will address the numbering plan, data tables, and data transfer required for conferencing in the GP network, as well as, interoperability with the SCP C^2 and RED Switch networks. The capabilities of the GP interoperation with the above networks is shown in Illustration 1-2 and will be further discussed in GP Conferencing Procedures (Paragraph 3.4).

3.1.1 Assumptions

1. All STU-III users will be able to be included in a GP conference, unless they are behind a manual PBX or do not have the appropriate security level
2. All STU-III users that have a CONFIDENTIAL or higher security level can initiate a GP conference, including those behind a manual PBX
3. The GP system will eventually be required to support over one million STU-IIIs

4. When CDs are bridged together, the CD serving as the secondary CD will not be allowed to bridge to another CD. In other words, tertiary bridging is not allowed

5. A single conferee is usually not brought in through a secondary CD

6. The GP CD must interface DSN as a PABX with precedence in dialing

7. Precedence will be passed to the CD by the AUTOVON/DSN network thus the CD will appear as a PABX to the network

8. GP conferencing will not support TS/SCI

9. GP CDs will be in a RED controlled area

10. Users authorized to initiate a specific preset conference are also given its precedence even if this exceeds the user's normal authorized precedence.

3.1.2 GP Security

The GP Conference Director will support CONFIDENTIAL, SECRET, and TOP SECRET conferences. However, in supporting multi-levels of security, other security issues arise. How will the CD be informed of the security level of the conference, and more importantly, what security level will each STU-III display and how will this differ from the actual security level of the conference?

Several limitations associated with the RIT currently exist that make it difficult or impossible to utilize all the features of the CD. If all conferences were to be held at a single security level, the procedure would be straightforward. However, when the CD supports multiple security levels, the process becomes more complicated and more difficult to achieve. The RIT/CD would at least need to provide the following functions:

1. A method for the STU-III conference originator to select the security level of the conference (up to his highest authorized security level)

2. A method for calling conferees at a specific classification level.

The conference originator must be able to select the security level of the conference. If this were not possible, a user with a TOP SECRET clearance would not be able to establish a SECRET or CONFIDENTIAL conference with conferees that are cleared only to those levels. This can be done in several ways:

1. The conference originator could initiate a conference by calling the CD and synchronizing with the RIT at the normal security level at which his STU-III operates. The RIT would then send a message to the CD indicating the classification of the connection. The conference originator could then send a code to the CD indicating the level at which the conference is to be established. The conference originator would be limited to the classification of the connection between the RIT and the originating STU-III. For example, if the originator and RIT are synchronized at the SECRET level, the originator could originate a SECRET or CONFIDENTIAL conference but would be prohibited from originating a TOP SECRET conference. The potential problem with this method is that the originator may be connected to the CD at a higher security level than the rest of the conferees. For example, the originator's STU-III would display SECRET while the rest of the conferees STU-IIIs would display CONFIDENTIAL. This means that the originator must remember throughout the conference to disregard the display on the STU-III and keep in mind the actual security level of the conference.

2. Crypto Ignition Keys (CIKs) could exist for all classification levels up to the highest a user is cleared for. At least one of the three commercially developed STU-IIIs provides such a feature. In this way a STU-III user cleared to the SECRET level would have two CIKs. One that allows for SECRET communications and a second that would

allow CONFIDENTIAL communications. This is a poor solution because not all STU III's being manufactured will support this and it would more than double the number of CIKs issued.

3. Set an entire CD to a specific security level and have the originator dial the CD with the desired security level of the conference. In this case, each STU-III would be given access to a CD at each security level at which it is authorized to operate. This may not use AUTOVON/DSN very well since, for example, a TS user would have access to three primary CD's and three alternate CD's which may be very far away.

4. Three RITs could be placed at each port of the CD, one at each of the three security levels and each with its own telephone number. This would solve the RIT and CD communication problem wherein once the CD is made aware of the conference classification, no automatic method exists for the CD to set the classification level of the RIT. The conference originator would then have to call one of the RITs set to the security level being called. For example, a STU-III user wishing to originate a conference at the SECRET level would call an RIT set to the SECRET level at his local CD. The CD would know that port has an RIT set to the SECRET level and that all conferees must be called through RITs at the SECRET level. This is the recommended way since it was AUTOVON/DSN resources better and STU III's are cheaper than CDs.

Ideally the RIT should perform the following functions:

1. Pass the classification level of a connection established with a STU-III to the CD

2. Have its security level set by the CD

3. Force a distant STU-III into the secure mode

Presently only the first of these three functions is supported.

3.2 GP NUMBERING PLAN

The DSN Worldwide Numbering Plan [1] will establish a standard numbering system that can serve all DSN users throughout the world in a uniform manner. The DSN numbering plan will be designed to be interoperable with the Worldwide AUTOVON Numbering Plan and the European Telephone System (ETS) Numbering Plan. The plan will have sufficient capability and flexibility to permit it to accomodate new DSN features, such as conferencing, without major changes. The following abbreviations will be used to designate the allowable range of digits:

Designation	Digit Range
X	0-9
Y	0-1
N	2-9
P (Precedence)	0-4

The numbering plan consists of precedence, route code, area code, switching center code, and line number. The precedence code can be any digit 0-4. The route code is a special purpose code which permits the customer to inform the switch of special routing or termination requirements. The three digit area code (NYX code) is unique to the major geographic areas (CONUS, Europe, Caribbean, Pacific, and Alaska).

The three digit switching center code (NNX) identifies and directs a call to the switch serving the called number.

The four-digit line number identifies the specific terminal in the called switching center.

A goal of the AUTOVON/DSN is to provide access to many features and services through a single line instrument. As the number of features increases and the methods of providing them become more diverse, it becomes necessary to provide standard methods of accessing the capabilities. While the recommended numbering assignments are not mandatory, the format will be adhered to in order to maintain network integrity and allow for expansion.

3.2.1 Precedence Dialing

GP conferencing will support precedence dialing by employing MLPP (see Appendix B). The precedence will be the first digits dialed when necessary and must be equal to or below the maximum allowable precedence that the originating STU-III is authorized. The desired precedence will be achieved by dialing one of the following numbers:

P =	90	FLASH OVERRIDE
	91	FLASH
	92	IMMEDIATE
	93	PRIORITY
	94	ROUTINE

Where seven digit local dialing is employed, the precedence code may be omited for ROUTINE dialing.

3.2.2 Maximum Calling Area (MCA)

The AUTOVON/DSN network does not forward the maximum calling area (MCA) through the network. When a request for an area code is received, the serving switch will act upon the request based on the originators classmarking within the switch. Controlling the maximum calling area after being connected to a conference bridge requires that either the maximum calling area must be included in the STU-III ID Field information or that the database within the conference node must identify the MCA associated with each user (discussed further in Paragraph 3.3.4.4).

3.2.3 Normal Dialing Format

Since GP is planned to be a capability provided by DSN, the dialing format will be the same as that in DSN. This dialing is used when calling a CD or a dingle conference. The dialing format is as follows: (P) (NYX) - NNX - XXXX, where (P) is the precedence of the call, (NYX) is the area code; NNX is the switch code, and XXXX is the line number. The symbols in parenthesis are not always dialed. This is further explained in DSN Switching Requirements manual.

3.2.4 Preset Conference Numbering

For preset conferences, the originating subscriber must first access his primary conference director (where the preset conference numbers are stored). Once the CD announces that it is ready to receive conference dialing information, the originator would enter the secure dialing mode and enter the preset conference code (XX) followed by end of dial code (#). The conference director would then dial all the subscribers listed in the preset conference database for that particular code. The preset code would be interpreted at the CD and not by AUTOVON/DSN.

3.3 GP DATA TABLES

The GP CD will contain or be given the necessary information to establish a preset or random conference. This information includes such things as the authorized precedence and the maximum calling area (MCA) for each subscriber assigned to the CD for conference origination.

This information will be stored in a set of data tables. The individual data elements will either be dynamic or static in nature. Static data elements are those which are resident in the CDs main or secondary storage. The CD always has access to this static data. Dynamic data elements are transfered to the CD from some other source (i.e., AUTOVON/DSN, STU-III, etc.) directly preceding the establishment of a conference. Dynamic data elements are only stored temporarily in the CD main memory.

3.3.1 Required Data

The GP CD requires the following data to establish a conference:

1. Terminal ID (Originator)
2. Originator's Authorization
   a. Maximum Allowable Precedence
   b. Security Level
   c. Conferencing

(1) Authorized random conference only

(2) Authorized preset conference only

(3) Authorized preset and random

d. Maximum Calling Area (MCA)

3. Preset conference data

4. Conference Set-Up data

5. Secondary CD data

6. GP Announcement (see Appendix C).

3.3.2 Data Acquisition Method

If all one million users are allowed to originate a conference, a method must be developed so that the CD can ascertain certain information about the user's authority for conference origination. For example, the CD must know what precedence level the conference originator is authorized and the user's authorized calling area classmark. Two possible solutions to this problem follow:

1. Store the authorization information in memory as was originally planned. If there were a limited number of STUs all this information could be stored in the CD. However, now with over a million users, it would be very time consuming to maintain all this information in the CD.

2. The GP CD could obtain authorization information (such as maximum allowable precedence) from a STU-III terminal during the secure call setup through the AUTOVON/DSN between the RIT and identified STU-III terminal. During this period, the terminals will enter a signaling sequence where the traffic key is generated and ID Field information is exchanged between both terminals. The additional information required by the CD could possibly reside in the STU-III ID Field (See Paragraph 3.3.5.1), since six seven bit characters are currently unused in the terminal ID Field. This information would then be passed from the RIT to the conference bridge,

where it could be accessed. If this additional information was to reside in the terminal ID Field, it would have to be incorporated into the keying information. Therefore, NSA would have to be responsible for programming this additional information into a unique terminal ID Field. The problem is that the space in the ID Field may not be sufficient to hold all the information required. Also, NSA may have other plans for this space or may not be willing to be burdened with the additional responsibility.

3.3.3 Recommended Data Acquisition Method

Neither of the single methods discussed above is ideal for all the data elements. However a combination of these techniques will lead to the best possible solution.

1. User ID (from STU-III)
2. Originator's Authorization
   a. Precedence (from AUTOVON/DSN)
   b. Security Level (from STU-III)
   c. Conferencing (from STU-III)
      (1) Authorized random conference only
      (2) Authorized preset conference only
      (3) Authorized preset and random
   d. Maximum Calling Area (MCA) (from STU-III)
3. Preset conference data (stored in CD)
4. Secondary CD data (stored in CD)
5. GP Announcements (stored in CD).

The following recommended data element acquisitions will be utilized in the remainder of this report relative to GP conferencing.

3.3.4 Data Element Description and Format

3.3.4.1 Terminal ID

The terminal identification for a STU-III-to-STU-III call would contain the division, department, and possibly the user name.

However, for several reasons, it is not recommended that the user name be included in the STU-III ID Field information. First, more than one person may be using or have access to a particular STU-III. In such a situation, associating a name with a terminal has little meaning. Second, personnel changes are made relatively frequently and department mission and requirements are relatively static. Every time there is a personnel change, the ID would have to be updated, but if a department moved locations, the STU-III could be simply taken to the new location without interrupting service.

In conferencing, the terminal ID cannot be used in the usual manner. This would require the RITs at the conference director to transfer the originator's ID to each conferee, but what ID would appear on the originators terminal? A possible solution might be to provide each RIT at a conference director with an ID that says "CONFERENCE." This would appear on all conferees' terminals as well as the originator's, but would not affect regular terminal ID display for two-party calls.

3.3.4.2 Maximum Allowable Precedence

The Worldwide Numbering and Dialing Plan establishes a standard numbering system that will serve all AUTOVON/DSN users throughout the world. Within the STU-III ID Field, the precedence digit is 0 for FLASH OVERRIDE, 1 for FLASH, 2 for IMMEDIATE, 3 for PRIORITY, and 4 for ROUTINE. As a result, the data format will require only one (1) character, which could also be represented with three (3) bits.

3.3.4.3 Security Classification

The security classification capability for the STU-III community of users will be UNCLASSIFIED, CONFIDENTIAL, SECRET, TOP SECRET, and TOP SECRET/SCI. During a secure call, the STU-III will display the highest mutual classification of the two terminals on the display window.

3.3.4.4 Conferencing Authorization

Three possible conferencing privileges exist which a STU-III terminal may be assigned for initiating a conference:

1. Authorized random conference only
2. Authorized preset conference only
3. Authorized preset and random conferences.

The format for this can be one (1) character or two (2) bits. Any GP STU-III user may be included in these conferences except for those not having the proper security level or behind a manual PBX.

3.3.4.5 Maximum Calling Area (MCA)

The current AUTOVON/DSN numbering plan has the world divided into five (5) distinct area codes: CONUS, Alaska, Pacific, Europe, and Caribbean. Representing all the possible combinations of allowable calling areas (32 total) would require two (2) characters, which could also be represented by five (5) bits.

3.3.4.6 Preset conference data

When an authorized STU-III requests a unique preset conference code, the serving CD will proceed to the lookup data table, which will identify the dialing sequence necessary to provide the conference connectivity. These preset conferences will be updated and changed by authorized maintenance/operations personnel. The format of the preset conference data is as follows:

Preset ID# (2 digits) 00-99		
Precedence*		(1) Character
Security Level*		(1) Character
Telephone Numbers	:	
1	:	Dialing Data
2	:	Dialing Data
3	:	Dialing Data
.	:	.
.	:	.
.	:	.
10	:	Dialing Data

* Security level and precedence can be changed by the conference originator at conference initiation time. However, originator's precedence and security level may not be exceeded.

Dialing Data Format

- switch code(NNX) + line number(XXXX)
- area code(NYX) + switch code(NNX) + line number(XXXX).

3.3.4.7 Secondary Conference Set-Up data

This data is required when a CD needs to bridge to a secondary CD. The first column "All NYX and NNX codes" is a list of all the NYX and NNX codes utilized in AUTOVON/DSN for serving users, exluding CDs and other special NNX codes. Each of these codes could be assigned to a primary CD and an alternate CD. In this way the originating CD could determine which users are served by which primary and alternate CDs. This also limits the access of the originating STU-III to one primary CD and an alternate, if necessary. The table could look as follows:

ALL NYX and NNX CODES	DSN ADDRESS OF PRIMARY CD	DSN ADDRESS OF ALTERNATE CD

The STU-III user may access the alternate CD if his primary CD is not available. The user will still be able to establish random and preset conferences, but the preset conferences at the alternate CD will probably be different than those in the primary CD.

3.3.5 STU-III Data Management

For STU-III conferencing, data management will encompass one million or more subscribers plus up to 60 to 80 conference directors. The current STU-III design calls for the terminal identification and security classification to be contained in the ID Field information. Current STU-III documentation states that the user identification could be by division, department, or specifically, the user name. As discussed earlier, it is identification of the STU-III by user name that would seriously impact data management.

Assume that the DCAOC in Arlington, VA has a validated requirement for five (5) STU-III terminals at different precedences, MCA, and security level. If the ID for each terminal merely displayed "DCAOC" and "SECRET," the COMSEC for the original activation would never require a change [as it would serve the mission requirement as stated in the Telecommunications Service Request (TSR) regardless of the personnel assigned within the DCAOC branch]. If the terminal ID contained information such as "DCAOC, MAJ JONES," the COMSEC would necessitate a change each time a personnel change occurred within the organization.

The impact of assigning the user's name as part of the terminal ID should be seriously considered within a network of one million subscribers. Is the users name essential to the day-to-day business dealings conducted by telephone? If your telephone rings and displays "DCAOC" "SECRET," once you go off hook the caller will identify himself. For identification purposes, it might be beneficial to ID the phones as DCAOC #1, DCAOC #2, etc., especially if they have different capabilities.

The security classification assigned to each terminal via the TSR process should remain constant and any updates or changes should be minimal.

3.3.5.1 Additional STU-III ID Field Information

If the STU-III also includes the maximum calling area, and conference authorization within the ID Field information, it should not seriously impact CD data management. These are assigned based on mission requirements rather than user requirements and should remain fairly constant once the requirement is validated and activated. This solution, however, would have an impact on the COMSEC management.

3.3.6 Conference Director Data Management

Under a scenario where the STU-III ID Field information would contain ID, security classification, maximum calling area, and conference authorization, the databases within the CDs would only be required to contain the preset conferences including authorized originators, a table of announcements, and data related to other CDs. All other classmarks and verification would be accomplished by the AUTOVON/DSN network and STU-III synchronization.

Under the scenario where the STU-III ID Field information contains only the ID and the security classification, the COMSEC data management becomes much simpler, while the management of the CD databases becomes somewhat more complex. The CD would be required to have data tables for user authorization and verification of MCA, and random and preset conferencing, in addition to announcements.

3.4 GP CONFERENCING PROCEDURES

In order to establish preset and random GP conferences, it is necessary to transfer data between the different elements that comprise the GP conferencing system. It is this transfer of data between components that brings about the desired connectivity and provides the conferencing capability. This section will discuss the data transfer from STU-IIIs to the CD, from the CD to STU-IIIs, and from CD to CD. In addition, conference setup procedures and interoperability with SCP C^2 and RED Switch networks will be discussed from the view point of the originator in GP as shown in Illustration 1-2.

3.4.1 Initial Connection to CD

Any STU-III user may gain access to the GP CD in the following way:

- User (originator) inserts CIK into STU-III
- User picks up handset
- User waits for dial tone (if behind a manual PBX the user must ask the operator for an outside line)
- User enters precedence of call
- User places a call to CD
- AUTOVON/DSN checks to see if the originator's classmark allows him the precedence entered and the number dialed is within his MCA
- AUTOVON/DSN connects originator to RIT/CD. If all lines to the CD are presently in use at equal or higher precedences then AUTOVON/DSN will give the conference originator a busy tone or an announcement. However, if any of these lines in use are of lower precedence, they would be preempted using standard MLPP precedures.

Note:

If AUTOVON/DSN preempts a line for a conference originator of higher precedence either a conferee or conference originator in a conference of lower precedence was preempted. AUTOVON/DSN will give the disconnected party a preemption tone. If a conferee was disconnected the CD will make an announcement to conference participants that the conferee is no longer a participant in the conference. If a conference originator was disconnected (either by being preempted or going on-hook), the CD must notify all participants that the conference is to be terminated. The CD has no way of knowing the difference between a preempted line or a participant hanging up his phone (see Appendix B).

- RIT synchronizes with the originating STU-III and enters secure mode if the security level of the STU-III is at least confidental

- STU-III transfers the following data to RIT: Terminal ID, Security Level, Conference Authorization, MCA
- RIT transfers the following data to CD: Terminal ID, Security Level, Conference Authorization, MCA
- The CD stores this data in temporary data tables
- User enters the secure dialing mode
- The STU-III enters the secure dialing mode with the RIT.
- User enters the code of the security level of the conference
- The CD verifies that the STU-III is authorized that security level

3.4.2 Entering GP Conference Data

Once the STU-III is in the secure dialing mode, the originator may establish a random or preset conference. If at any time the originator exceeds his authorized classmark, the CD will return the appropriate announcement or tone (see Appendix C).

3.4.2.1 Random Conference

The following procedures are recommended in order to establish a random conference:

- User dials full address of first conferee
- If the user has dialed a correct address, we recommend that he dial (*) to signify completion of a correct address. The user may then proceed with other conferees in a similar manner
- If the user dials an incorrect address, he may delete this address by dialing (#), as long as the completion of correct address (*) had not been dialed for that address
- The CD checks to see if the desired call is within the user's MCA

- After dialing (*) for the last complete correct address, the user dials (#) to signify end of dialing.

3.4.2.2 Preset Conference

The following procedures are recommended in order to establish a preset conference:

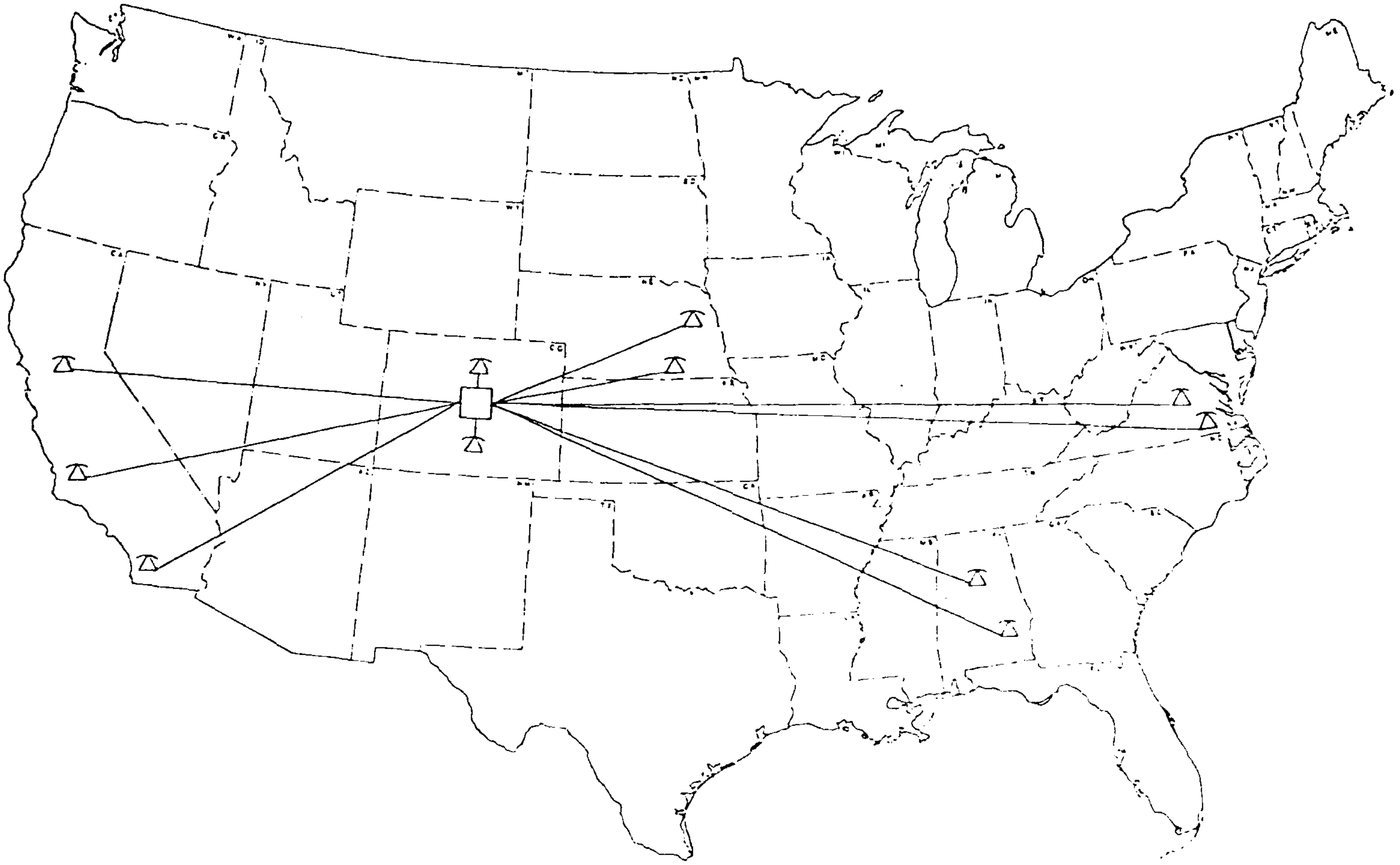
- User dials two digit code for the desired preset conference
- User dials (*) after correct code or (#) to delete an incorrect code
- CD checks to see if the user is authorized to originate the desired preset conference (the CD does not check if the preset conference default precedence is higher than the originators)
- The user may then dial additional random conferees using the same procedures described above for a random conference
- The CD will check to see if each additional conferee is in the user's MCA
- The user dials (*) after the last correct entry, then dials (#) to signify end of dialing.

3.4.2.3 GP CD Bridging

Conferences should be established in such a manner as to have minimum impact on the AUTOVON/DSN network. For example, if a user in Colorado wishes to establish a conference with the conferees shown in Figure 3-1 there are several ways in which the conference could be established. These are not discussed in the A SPEC but may be advantageous to look at.

1. The first and simplest method (Alternative #1) is to have the conference originator's local CD call all the conferees directly. This would result in a star configuration similar to Figure 3-1.

Figure 3-1. Example Conference Connectivity with Alternative #1



2. A slightly more complex, but more efficient, method (Alternative #2) connects the conferees to a more local CD and then bridges these CD's to the originating CD. This configuration is shown in Figure 3-2.

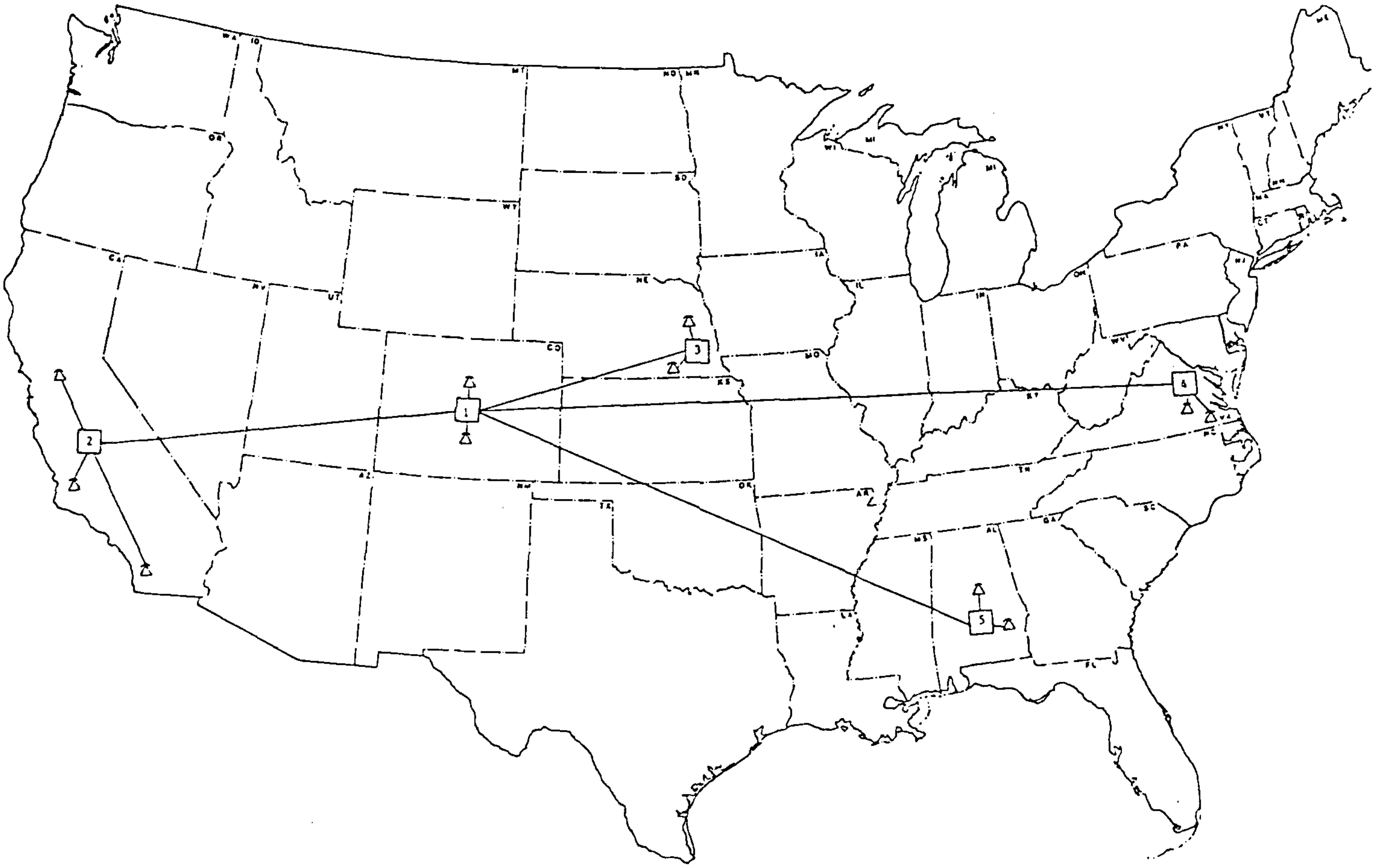
Alternative #2 makes no limit on the number of secondary CDs a primary CD can bridge, with the exception that it is contingent upon the number of ports of the primary CD. Alternative #2 makes the most efficient use of AUTOVON/DSN facilities, but this alternative does not necessarily use conferencing facilities optimally. For example, in Figure 3-2 the primary CD (#1) in Colorado has brought in 10 conferees-one locally, and 9 through other CDs. In this configuration the following conferencing resources where used:

CD #1	-	3 Ports
CD #2	-	4 Ports
CD #3	-	3 Ports
CD #4	-	3 Ports
CD #5	-	3 Ports
Total		16 Ports

If the primary CD had brought in all these conferees directly (as in Alternative #1), only 11 ports would have been used, a difference of five ports. A single such occurance may not seem significant but many of these conferences operating simultaneously may quickly utilize most of the ports on CDs throughout the conferencing system.

In summary, Alternative #1 uses AUTOVON/DSN resources poorly and conferencing facilities most efficiently, and Alternative #2 uses conferencing facilities poorly, but uses AUTOVON/DSN the most efficiently. Assuming that both AUTOVON/DSN and conferencing facilities are equally precious resources, a third Alternative has been developed.

Figure 3-2. Example Conference Connectivity with Alternative #2



3. The third-and most complex-method (Alternative #3) uses both AUTOVON/DSN and conferencing facilities relatively efficiently by using a topological design algorithm to calculate the most efficient manner in which a conference is to be configured. The CD using this algorithm will determine in real-time the optimal or near optimal configuration for the conference upon completion of dialing data from the conference originator. A possible configuration that may be chosen by the algorithm is shown in Figure 3-3. Alternative #3 attempts to strike a compromise and use both AUTOVON/DSN and secure voice conferencing facilities relatively efficiently.

The recommended selection criteria and characteristics of such an algorithm follows:

1. Determine if any of the desired conferees are not located at the originator's home switch

2. Bring in two or more conferees in any of the following areas (CONUS, Pacific, Europe, Alaska, Caribbean) by at least one CD

3. If two or more conferees are in any of the following intra-area divisions, bring them in using a secondary CD, if possible, otherwise bring them in directly:

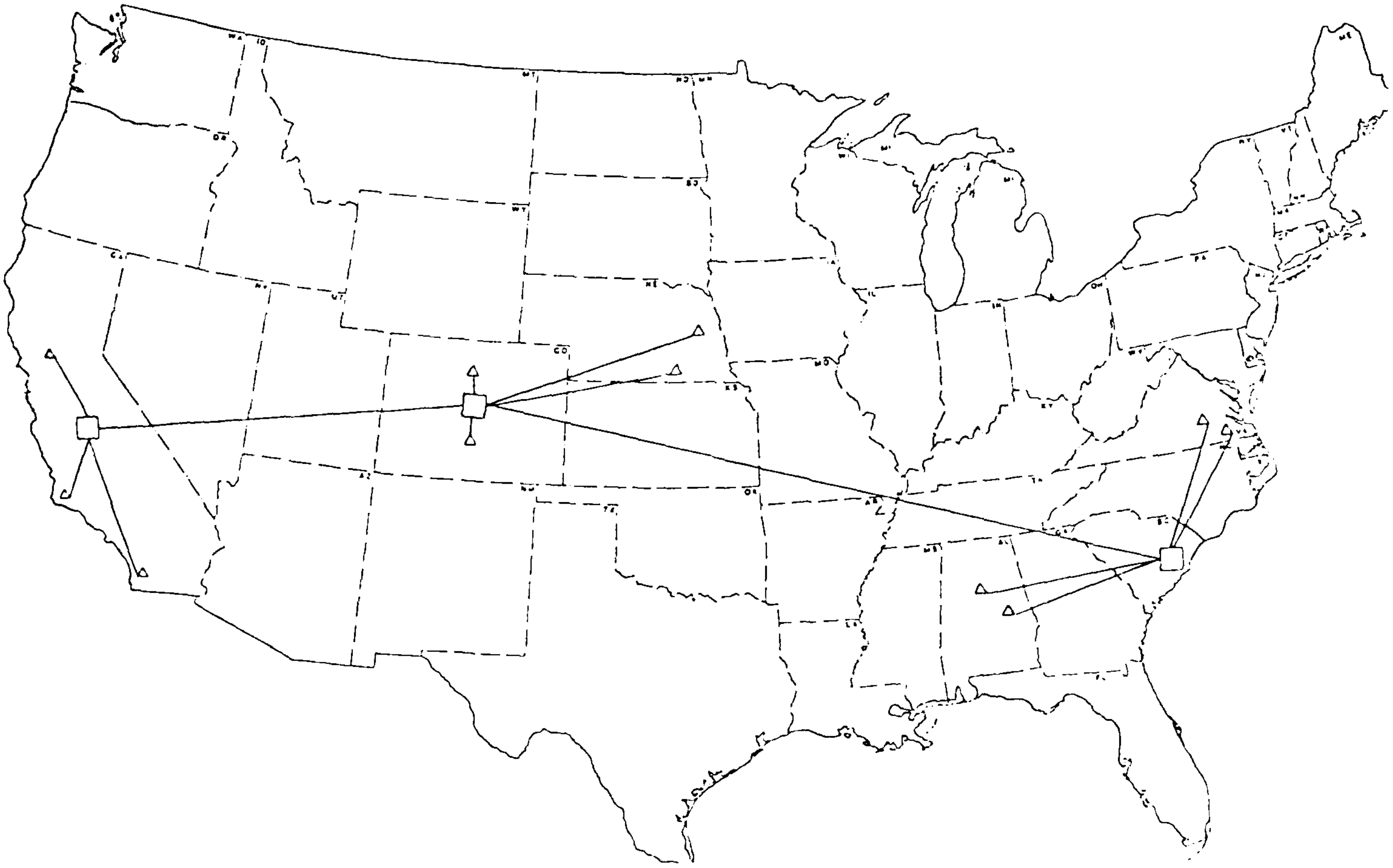
   Europe - England, Germany, and Mediterranean
   Pacific - Hawaii, Japan/Korea, Philippines/Guam

   CONUS - no set geographical divisions, but should probably have three to six logical divisions that are determined by the algorithm on a per conference basis

   Alaska - None
   Caribbean - None

- Calculate configuration in real-time

Figure 3-3. Example Conference Connectivity with Alternative #3



- Compensate for CDs that are not available by going to at least one alternate CD or bring in the conferees at the nearest CD already being utilized in conference; however, this could cause a problem with long time delays in conference set-up. Therefore, a time limit should be set at which the originating CD will abandon trying to call a secondary CD and just dial the necessary conferees directly.

When the conference originator has completed entering dialing data and the CD has determined that one or more secondary CDs are required to set up the conference the following occurs:

- The primary CD establishes a connection with the secondary CD by calling the appropriate secondary CD through an RIT and AUTOVON/DSN. If more than one secondary CD is to be bridged, the primary CD will have to call each one individually
- AUTOVON/DSN connects the primary CD/RIT to the secondary RIT/CD using the standard MLPP procedures
- Once the two RITs have been connected, the primary CD's RIT transfers the following data to the secondary RIT: terminal ID (containing RIT/CD ID), security level, conference authorization, and MCA (Note: conference authorization and MCA are transferred, but are meaningless in secondary conferencing; the primary CD will check the authorization and MCA of any data sent to the secondary CD)
- When the RIT of the primary CD and the RIT of the secondary CD synchronize, the primary CD instructs its RIT to go into the secure dialing mode
- The primary CD sends the secondary CD a code indicating that a primary CD wishes to establish a secondary conference

- The primary CD transmits the dialing information to the secondary CD
- The already-established connection between the primary and secondary CD will be utilized to bridge the CDs together
- The secondary switch will store the numbers of unanswered or busy lines for possible retry and also transmit the numbers back to the primary switch for possible retry by the originator.

Note: The primary and secondary conference directors should always exit the secure dialing mode when not transmitting data to another CD. If a CD goes into the secure dialing mode to send a message to another CD during an on-going conference, the secondary CD will temporarily be cut off from the conference. ıf the secondary CD goes into the secure dialing mode, the conferees at the secondary CD will temporarily only be able to listen. If the primary CD goes into the secure dialing mode (rare during a conference), the conferees at the secondary CD will be able to speak but not listen. The exact length of the interruption is not presently known, but it is expected to be less that 1/2 second. Also, the secondary CD will appear as a single conferee to the primary CD. This makes it more difficult for a conferee at the secondary CD to gain speaker control since there will be two stages of contention to go through, first at the secondary CD then again at the primary CD.

3.4.3 GP STU-III Use of RED Switch Confeɛrence Bridge

Appropriately classmarked, GP STU-III users will be able to access the RED Switch conference bridge through the RED Switch attendant. These GP STU-III users must have at least a SECRET security classification and all conferences including the RED Switch conference bridge will have to be held at the SECRET level. The RED Switch will block any classification less than SECRET. There are two ways that the authorized GP STU-III user can use the RED Switch conference bridge.

3.4.3.1 Direct Access

Certain GP STU-III users will be authorized to initiate a conference on the RED Switch conference bridge as follows:

- STU-III user inserts CIK (must be able to operate at SECRET level or higher)
- User picks up handset
- User waits for dial tone (if behind a manual PBX, the user must ask operator for outside line)
- User enters precedence of call
- User places a call directly to the RED Switch attendant
- The RS/RIT and STU-III synchronize and transfer data (as in Paragraph 3.4.1)
- The RS attendant verifies the calling STU-III is authorized to originate a RED Switch conference (Note: ıt is not clear how the attendant determines if the conference originator is authorized, since the GP CD passes no information about the originator to the RED Switch)
- The user then gives the attendant the necessary conferencing information
- The attendant checks the conference information, assuring that the user is not exceeding his classmark
- The attendant then follows the procedure to initiate a conference, as discussed in Paragraph 5.4

- If more than one STU-III is included, the RED Switch Digital bridge will automatica'ly be used if available for the STU-III participants
- The attendant may give the originator's authority to a RED Switch user in the conference
- The RED Switch conference will operate in the speaker/broadcast mode based on the STU-III interface trunk classmarks.

3.4.3.2 Access Through GP CD

GP STU-III can also access the RED Switch by going through the GP CD, as follows:

- STU-III user gains access to the GP CD as described in Section 3.4.1
- STU-III originator dials the necessary conference information as described in Paragraph 3.4.2
- The GP CD would access each RED switch user through a RED Switch/STU-III interface trunk and appear to be just another STU-III to the RIT/CD
- Alternately, If more than one user at a single RED Switch is required, the RED Switch attendant for that switch may be included as an initial conferee
- After the GP conference starts, the RED Switch attendant would setup a secondary RED Switch conference according to originating STU-III instructions
- Once the secondary conference is established the RED Switch attendant would connect it to the trunk from the originating CD.

3.4.3.3 Bridging a GP CD to the RS Analog Conference Bridge

Bridging of the RED Switch conference bridge and the GP CD can only be done by the RED Switch attendant. In order to do this, the originating STU-III would include the RED Switch attendant as an original conferee. Then the attendant would set up a secondary conference in the RED Switch and connect it to the trunk from the GP CD as follows:

- AUTOVON/DSN connects the primary CD/RIT to an RIT at the RED Switch using the standard MLPP procedures
- Once the two RITs have been connected, the primary CD transfers the following data to the RED Switches' RIT: terminal ID (containing RIT/CD ID), security level, conference authorization, MCA (Note: conference authorization and MCA are sent but are meaningless in secondary conferencing; the primary CD will check the authorization and MCA of any data sent to the RED Switch)
- When the RIT of the primary CD and the RIT of the secondary conference synchronize, the RED switch will ring the RED Switch attendant's phone
- The conference originator will then be able to verbally explain his needs to the RED Switch attendant
- The RED Switch attendant determines whether the request is valid and whether the originator has the authorization (Note: it is not clear how the attendant determines if the conference originator is authorized, since the GP CD passes no information about the originator to the RED Switch)
- Assuming the attendant honors the originator's request, he does the following:

  1. Obtains the line numbers (or names) of the conferees at his RED Switch (conferees at other RED Switches must be called through their RED Switch)
  2. Connects them to the bridge, if available (the bridge is not used if only one conferee is available)

3. Connects the bridge or single conferee to the line that presently connects the GP CD and RED Switch attendant (if the bridge is used it will automatically revert to the speaker/broadcast mode when bridged with a GP CD).

   Note: Once the RED Switch attendant has transfered his connection with the GP CD to the bridge or single conferee he can only be reached by being called on a separate line.

3.4.4 GP STU-III Use of C^2 CD

GP STU-IIIs will not be able to access the C^2 CD. If necessary, the GP STU-III user could call a single C^2 STU-III through the AUTOVON/DSN network, and include him in a GP random conference.

3.4.5 Conference Set-Up and Modification

Once the user signals end of dialing, the CD will decide which conferees will be dialed directly and which will be setup on a secondary conference. This will already be established for preset calls. The CD then checks to see if there is a sufficient number of ports to support the desired conference. The CD will exercise MLPP procedures when necessary. If there are still not enough idle or preemptable ports to complete the desired call, the CD will return a busy signal to a ROUTINE originator or a "Blocked Precedence" announcement to an originator above ROUTINE. Once a sufficient number of ports are seized by the CD, it will dial the necessary numbers to setup the conference.

3.4.5.1 Conference Start

The conference will start when one of the following conditions is met:

1. All conferees have been connected and informed by an announcement that this is a conference call. This will take only a few seconds after the last conferee answers.

2. The designated period of time has elapsed (equivalent of 10 ROUTINE ring cycles) and conferees have answered or been determined not available. Busy or unanswered numbers will be temporarily stored for possible retry.

3.4.5.2 Conference Modification

The conference originator is the only conferee who can make modifications. The conference originator can add or delete conferees and transfer the originator status by entering the secure dialing mode and entering the proper code and telephone number of the conferee. Conference origination can only be passed to a conferee connected to the primary CD.

If the CDs are bridged and require the exchange of conference data, they must set their RITs to the secure dialing mode and transfer the data. If the secondary CD wishes to send a message to the primary CD, the secondary CD puts its RIT in the secure dialing mode, sends the message, and exits the secure dialing mode. This will temporarily cut off the secondary conference. If the primary CD wishes to send a message to the secondary CD, the primary CD puts its RIT in the secure dialing mode, sends the message, and exits the secure dialing mode. This could cause a brief interuption of approximately half a second.

3.4.5.3 Conference Termination

The conference will be terminated under the following conditions:

1. The conference originator goes on-hook or is preempted without transfering originating authorization to someone else. The CD will notify all conference participants that the conference is terminated.

2. The entire conference is preempted by a higher precedence at the primary CD. Preemptions of a secondary conference will not terminate the rest of the conference, but a preempt tone will be sent to all other participants to inform them of the preemption.

SECTION 4 - SCP C^2 CONFERENCING

4.1 INTRODUCTION

The SCP C^2 will provide a survivable, flexible, responsive, secure voice and graphics communications capability to the National Command Authority (NCA) and the Unified/Specified CINCs in support of strategic decisionmaking command and direction during global or regional crisis situations. The SCP C^2 conferencing will be provided to major command centers through Digital Conference Directors (CDs) which utilize the Jam Resistant Secure Communications (JRSC) portion of the Defense Satellite Communications System (DSCS) Electronic Counter Countermeasures (ECCM) channel one transponder. Fully distributed, user-controlled voice conferencing, two-party secure voice calls, and secure graphics (facsimile and teletype) conferencing will be provided to the designated C^2 users, who consist of directly connected C^2 subscribers, remote C^2 subscribers, and RED Switch subscribers. Conferencing (secure voice and graphics) will be provided intra- and inter- node, and intra- and inter-satellite area between two or more parties.

Not only will SCP C^2 conference nodes be allowed to establish conferences over independent DSCS satellite channels, but the SCP Conference Directors (CDs) will provide access to the planned and existing terrestrial communications assets of AUTOVON/DSN. This will allow the SCP C^2 system to have enhanced redundancy and survivability through the use of alternate paths through the terrestrial network. This will also allow GP STU-III and RED Switch users to participate in a C^2 conference, if required. In addition, certain designated remote C^2 STU-III users will be allowed to establish intra-node conferences through the SCP CD.

The SCP C^2 conferencing system is scheduled to evolve from the Early Operational Capability (EOC) to the Final Operational Capability (FOC) between 1991 and 1995. EOC is separated into two phases. Phase I (which began in 1985) uses Navy-developed Advanced Development Model Digital Conference Directors (ADM-DCDs), Multiple Rate Voice Terminals (MRVTs), graphics terminals, and JRSC spread spectrum modulation equipment to introduce secure voice and graphics conferencing to eight command centers in the PACOM area through the WESTPAC DSCS II satellite. Phase II will extend this capability to a total of three satellite areas serving eight CONUS command centers and four European command centers.

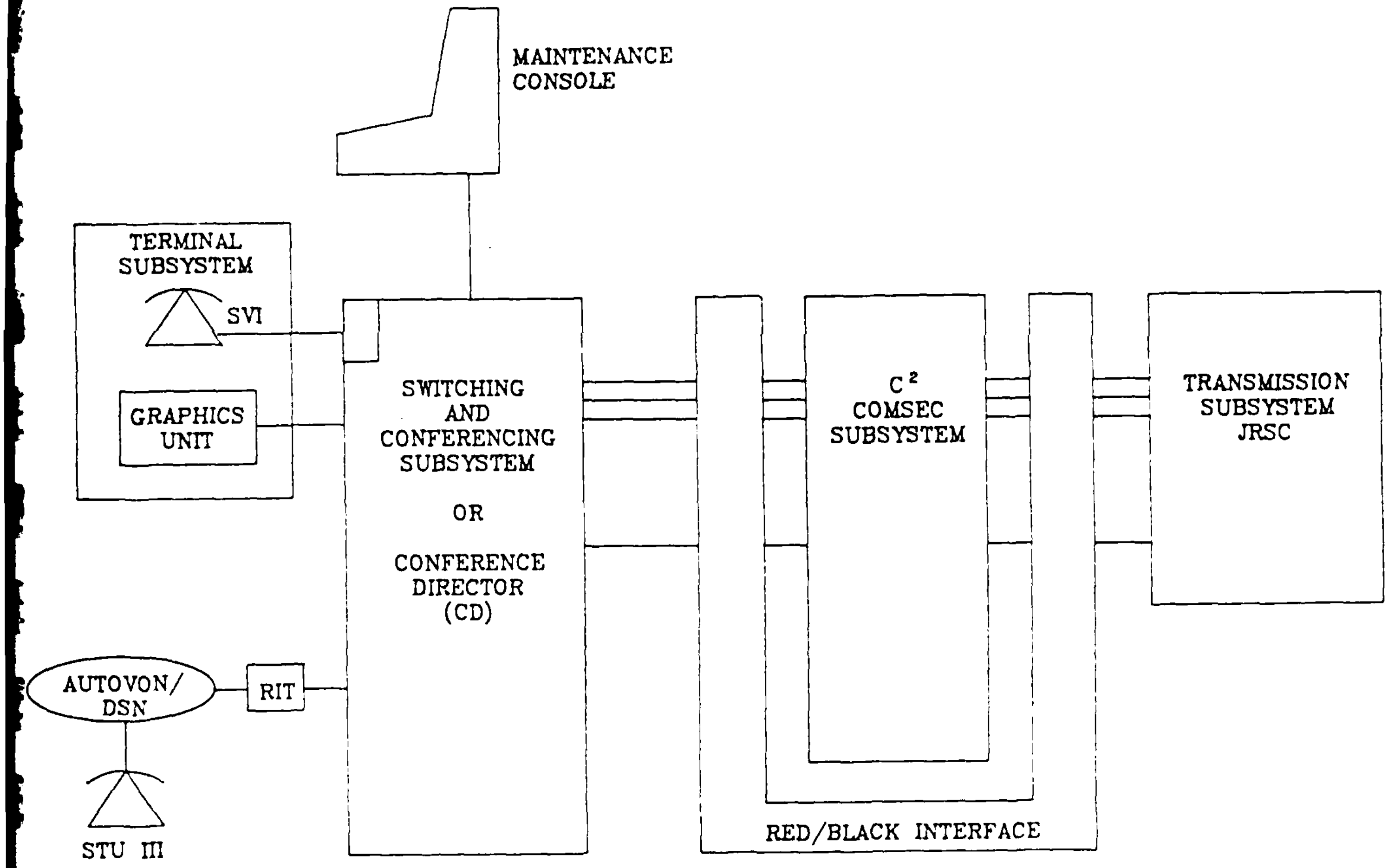
The SCP C^2 FOC will extend the conferencing capability to five satellite areas. Conferencing service to designated C^2 users will be provided through four subsystems of the C^2 Functional Element [5], shown in Illustration 4-1. These are the User Terminal Subsystem (UTS), the switching and conferencing subsystem or Conference Director (CD), the COMSEC Subsystem, and the transmission subsystem.

The UTS consists mainly of the end-user voice and graphics terminal equipment. The primary subscriber instrument will be the Secure Voice Instrument (SVI). The SCP CD will be the hardware and software, which provides the secure voice and graphic conferencing capability to C^2 users by serving as the CD. At this time, the SCP FOC CD is specified functionally but has not been designed.

For the SCP C^2 system, the number of active nodes will be limited to a maximum of 20 for each of the five DSCS satellite coverage areas. Some of these nodes will serve as relays between satellite areas.

This section will address the numbering plan, data tables, and data transfer required for conferencing in the SCP C^2 FOC network, as well as interoperability with the General Purpose (GP) and the RED Switch network. The FOC capabilities of the SCP C^2

Illustration 4-1. SCP Node Configuration



interoperation with the above networks is shown in Illustration 1-2 and will be further discussed in SCP C^2 Conferencing Procedures (Paragraph 4.4).

4.1.1 Assumptions

The following assumptions were taken in developing the numbering plan, data tables, and data transfer required for conference setup:

1. All SCP C^2 subscribers are at least TOP SECRET security level
2. SCP C^2 will not support any security level below SECRET
3. There will be a Network Control Channel (NCC) in SCP FOC for transfering the required information between conference directors
4. There will be up to twenty (20) CDs per satellite area in the FOC configuration
5. The SCP CD will contain the three digit code "NNX," signifying each RED Switch in the CD's data tables.
6. SCP FOC design based on SCP Type A SPEC [7]
7. SCP C^2 CDs will have the appropriate level of software security.

4.1.2 Transition from SCP C^2 EOC to SCP C^2 FOC

The transition from SCP EOC to SCP FOC should occur between 1991 and 1995. Currently, the major concern is whether or not the SCP C^2 EOC equipment/software and procedures will be incorporated into the SCP C^2 FOC design. For example, a separate analysis[4] was conducted of the SCP EOC Phase I test results and found that the EOC system may not meet the FOC call establishment time. The bounds of this requirements are that not more than 20 nodes and less than 40 participants, regardless of geographic location, must be able to be connected in a preset conference in a certain time period. This time period is measured from the instant the participating nodes are configured for conference operation, providing that upon going off-hook, conferees will receive at least one cycle of a conference alerting message. This area of concern deals directly with the operation of the NCC. The EOC NCC is a dedicated, full period, Time Division Multiple Access (TDMA) channel. Each node in the satellite is assigned a time slot consisting of sync and crypto preambles and status messages. It provides the path to establish, alter, or terminate conferences. Because the EOC NCC cannot establish a conference in the FOC time period requirement, a new signaling design for FOC needs to be explored.

In addition, COMSEC operation may be different in the FOC. In the EOC, a common key is used in each satellite area. All NCC transmissions are received by all CDs on the same satellite channel with the same crypto key. Whereas, for the FOC, a centralized key distribution system will probably be employed in which per-call key variables will be distributed over the NCC only to desired conference participants.

All of the aforementioned concerns affect the eventual transition from EOC to FOC. A successful phase-in from EOC to FOC operation will depend on the degree to which the FOC system is compatible with the EOC system.

4.1.3 SCP C^2 Operational Concept

The SCP system will be a distributed network of conference directors that control, manage, and process secure voice and graphics conferencing in a worldwide network. The CD at each node will control of conference establishment, conference conduct, network control, and reconfiguration, as well as the signaling and supervision to communicate conference control parameters to other CDs in the network. Each CD will send these parameters over a channel termed the Network Control Channel (NCC).

The SCP C^2 system will be designed to implement multilevel precedence and preemption and will employ fast switching techniques utilizing a speaker/broadcast protocol for operation of a conference. Once the channel is acquired by a conferee, he has the channel until he stops talking, at which time the channel can be acquired by another conferee (after a holdover time).

Because of this fact, the JRSC modems, the cryptos, and the CDs must resynchronize on each transmission. If two or more speakers at different nodes begin talking within one satellite delay time (260 ms) of one another, contention can occur. Once contention has occurred, either a recorded announcement or a special tone will be sent to the voice instrument from the conference director to notify the conference participants.

4.1.3 Terrestrial Backup

As previously mentioned, AUTOVON/DSN will be the backup system for the SCP C^2 system in the occurence of failure or heavily degraded performance. Each SCP node will have the capability to terminate a maximum of 12 AUTOVON/DSN channels. Possible failure and degraded performance in the SCP C^2 system could result from any of the following events: outages, badly degraded performance in the DSCS ECCM segment, prolonged out-of-sync conditions (e.g., loss of synchronization in the terrestrial segment, loss of modem synchronization, loss of crypto synchronization), or intolerable delays in voice conferencing.

In the event of such situations or other breakdowns of the system, there exist three possible courses of action for an SCP C^2 subscriber:

1. Use the SCP C^2 conference director to secure a connection to the nearest operational C^2 conference director using AUTOVON/DSN. Then, acting as a remote C^2 subscriber to a CD, the C^2 subscriber at the damaged node would have the ability to originate a conference at

that node. This scenario is contingent upon the assumption that the SCP C^2 system is still operational over the DSCS ECCM segment and that the failure was a local failure associated with the subscriber node. In order to access another SCP C^2 CD, a unique authorization code would be assigned to each authorized user. Each conference director will have to keep updated in its memory a list of all authorized C^2 subscribers located at other SCP C^2 nodes who have the ability to utilize that C^2 node in event of failures, it would probably be easier if such information was placed in the RIT ID Field as in GP conferencing. It is also recommended that those authorized C^2 users have the FLASH (or even FLASH OVERRIDE) capability. It is recommended that the number of C^2 subscribers with this capability be small so as not to override the system.

2. Use the RED Switch if the SCP C^2 subscriber has access to one or if the C^2 subscriber is already located in the RED enclave. This would allow the C^2 subscribers, if authorized, the ability to initiate a desired conference using the RED Switch analog bridge which would call in other C^2 subscribers at other locations through the RED Switch.

3. If the C^2 subscriber has access to a STU-III that can utilize the resources of AUTOVON/DSN, the subscriber could try to originate a conference using the GP conferencing system. This would require that C^2 subscriber's STU-IIIs are authorized to use GP conference facilities. GP conferencing operation is described in Section 4.

It is recommended that the highest priority C^2 subscribers be given the ability to utilize any of the aforementioned approaches in the occurence of failure of his SCP C^2 operation. The best approach would be the first one mentioned, in which the C^2 subscriber acts as a remote C^2 subscriber to another SCP C^2 conference director. The reason is simple: the SCP C^2 system utilizes the resources of the DSCS ECCM JRSC segment, and this system will be more survivable than AUTOVON/DSN. Although this approach also involves using AUTOVON/DSN, it is assured that the AUTOVON/DSN terrestrial connectivity to another conference director will be of short distance and will involve limited AUTOVON/DSN assets while still allowing the C^2 subscriber to utilize the survivable satellite network.

4.2 SCP C^2 NUMBERING PLAN

The SCP FOC numbering plan will be simple, efficient, and have the capability to support all SCP nodes in five (5) satellite areas. The numbering plan shall include necessary features for interoperability with external networks and secure voice facilities such as the RED Switch. The numbering plan described herein is based on the SCP EOC [5] numbering plan, except it has been modified to support the extra satellite area, the additional SCP C^2 nodes, and interoperation with other networks and secure voice facilities. This numbering plan will be flexible enough to adapt to a maximum of twenty (20) conference directors per satellite area.

Within the numbering plan, the following abbreviations are used herein to designate the allowable range of various digits within the numbering plan:

Designation	Digit Range
X	0-9
S (Satellite)	0-9
N	2-9
M	2,3,8
P (Precedence)	0-4 (STU-III) (FO,F,I,P)

4.2.1 Precedence Dialing

The first digit to be dialed will normally be the precedence digit, when required. If the conference precedence is not supplied by depressing one of the precedence keys, then the CD shall assign the default precedence of ROUTINE. The entry of precedence, within the users classmarked capability, shall be designated by depressing one of the four following precedence keys:

P =	FO	FLASH OVERRIDE
	F	FLASH
	I	IMMEDIATE
	P	PRIORITY

If a C^2 user has a telephone that does not have the precedence keys (FO, F, I, P), then the user may use the DSN format by dialing nine (9) followed by a precedence digit as follows:

P=	90	FLASH OVERRIDE
	91	FLASH
	92	IMMEDIATE
	93	PRIORITY

4.2.2 Access Codes

Access codes shall be employed to give access to other networks. These codes shall be of the form "8X." The CD shall screen the received access codes against the users authorized capability. For example, all SCP users may not be able to initiate conferences into the RED Switch. At least the following three network services would be required for allowing a secure voice interoperability capability:

Access Code	Network/Service
86	SCP Network
80	RED Switch Network
83	DSN/STU-III

4.2.3 Local Dialing Format

The local numbering plan shall include a four-digit line number for establishing intra-node calls. The number assignments shall be of the form XXXX. Access to the local operator at the conference director shall be provided by dialing zero (0).

4.2.4 Normal Dialing Format

This dialing format shall be used when either establishing random conferences or making direct calls. The format for this type of dialing is shown in Illustration 4-2. After dialing the precedence, the next two digits dialed will correspond to the special access code. These codes will provide access to both SCP and other secure voice networks. The next three digits dialed will correspond either to the SCP node number, the RED Switch number, or AUTOVON/DSN number, depending on which access code was dialed. The special access codes are given in Paragraph 4.2.6. As already mentioned, the first digit "N" (if the node sequence is selected) shall be any number between two (2) and nine (9). The second digit of the sequence "X" corresponds to any number between zero (0) and nine (9). The third digit of the sequence shall represent the satellite coverage area (or areas if a relay node). The digits corresponding to satellite areas are given in Illustration 4-3. The last four digits of the dialing sequence correspond to the specific line number.

When dialing into the RED Switch network, after dialing the RS access code, the next three numbers dialed will be the RS number "NNX." The last four digits dialed will correspond to the line number in the particular RED Switch enclave.

4.2.5 Preset Dialing Format

Illustration 4-4 presents the preset dialing format. This is the dialing format to use when initiating a preset conference. The first digit dialed is the precedence. After dialing the precedence, the special feature code "#" should be dialed to

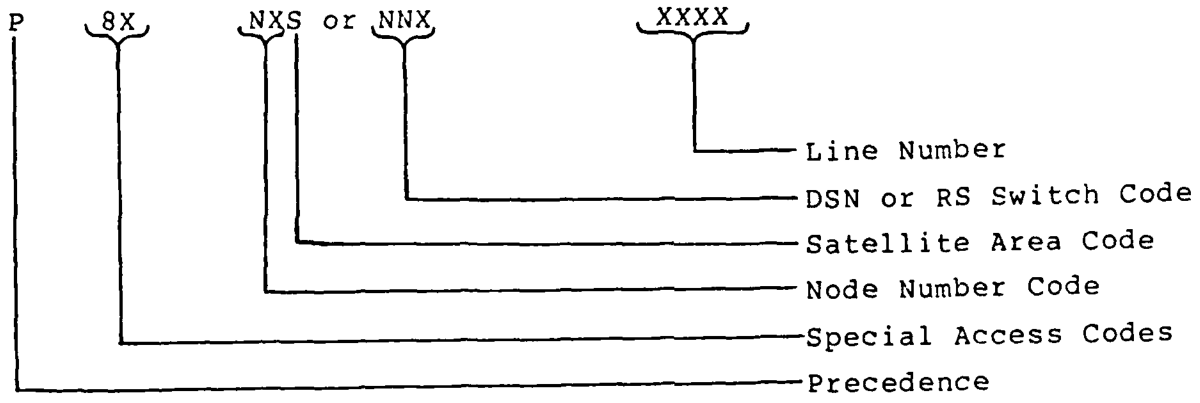


Illustration 4-2. Format for Normal Dialing

S =	0	West Pacific (WPAC)	
	1	East Pacific (EPAC)	
	2	East Atlantic (ELANT)	
	3	West Atlantic (WLANT)	
	4	Indian Ocean (IO)	
	5	WPAC/EPAC	Relay
	6	EPAC/ELANT	Relay
	7	ELANT/WLANT	Relay
	8	WLANT/IO	Relay
	9	IO/WPAC	Relay

Illustration 4-3. Satellite Area Designated Codes

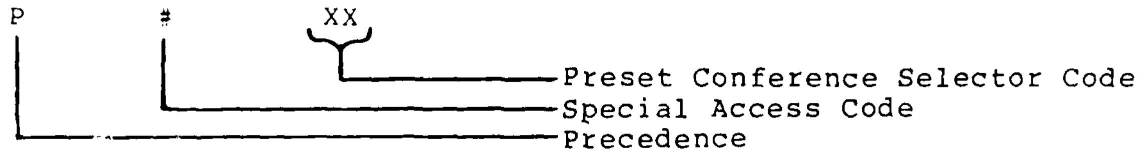


Illustration 4-4. Format for Preset Dialing

signify to the conference director that a preset conference format has been selected. The last two digits dialed will correspond to the number designated to represent a specific preset conference. After these digits have been dialed, the CD will proceed with the preset conference establishment process as described in Paragraph 4.4.

4.2.6 In-Conference Special Codes

Certain SCP performance requirements include the ability to add conferees, delete conferees, and transfer originator status. There will exist in the SCP numbering plan a set of codes which will allow the originator of a conference the capability to perform any one of the aforementioned requirements. These codes are given in Illustration 4-5.

These codes can only be initiated by the originator.

4.3 SCP C^2 DATA TABLES

This section will describe the data which must be contained in the conference directors in order to allow subscribers the ability to originate and participate in preset and random conferences. This data will be stored in a set of data tables.

The CD software shall possess the information required to control voice and graphics in a distributed network, between subscribers and satellite interfaces, and in relay CDs between satellite areas. These conference control functions will allow the CD to monitor subscriber status, satellite channel status, control traffic distribution, and conference information for status reports. The following paragraphs describe the data elements and tables which must exist in the conference directors in order to allow the CD the capability to control and manage conferencing both within the SCP network and for conferencing with RED Switch and GP networks and facilities. These paragraphs will only present the data tables required in the conference director. Paragraph 4.4 will describe the data transfer required among the SCP network elements.

M =	2	Add a Subscriber
	3	Delete a Subscriber
	8	Transfer Originator

Illustration 4-5. Special In-Conference Code

Data to be stored internally in the conference director will fall into one of three categories: static, semi-static, dynamic.

4.3.1 Static Data Table

The Static Data Table contains that information residing in memory at each node which shouldn't need to be modified. It is standard information defining the particular conference director. The following data, along with recommended storage space, shall make up the static data table at each node:

1. Node ID (2 characters)
2. Satellite Area ID (1 character)
3. Network Size (2 characters)
4. NCC Slot Position (2 characters).

4.3.2 Semi-Static Data Tables

Semi-Static Data Tables pertain to the tables that consist of data elements residing in the conference director which can be modified and updated via the CD operator entry interface. The operator interface shall be via a keyboard printer. The CD operator shall enter startup and hardware configuration data into the CD. In addition, the CD operator will enter the appropriate updated preset conference list information and parameters. Semi-static data tables maintained in the CD will include the following:

1. Preset Conference Table
2. Local Configuration Table
3. Satellite Configuration Table
4. Authorized C^2 Terminals (at other Nodes) Listing
5. PN Code and KG Crypto Key Tables
6. RED Switch Data Information Table.

4.3.2.1 Preset Conference Table

The preset conference table will include all of the preset conference lists. These preset conference lists will be updated and modified by the CD operator. SCP FOC design requirements specify that a node shall accommodate a maximum of 50 preset conference lists with up to 12 conferees in each list. The format of the preset conference list is as follows:

Preset ID# (2 digits)		00-99
Precedence*		(1) Character
Security Level*		(1) Character
Telephone Numbers	:	
1	:	Dialing Data
2	:	Dialing Data
3	:	Dialing Data
.	:	.
.	:	.
.	:	.
12	:	Dialing Data

* Precedence and security level may be changed by conference originator at conference initiation time. The originator's precedence and security level may not be exceeded.

4.3.2.2 Local Configuration Table

The data elements that make up the local configuration table contain information on the terminals (either remote or direct) that are attached to the CD. In addition, all of the line numbers and maximum allowable precedence of the terminals in the nearby located RED Switch SCIF will be stored in the SCP CD local configuration table. The data elements include the following:

1. Terminal ID
2. Maximum Allowable Precedence.

4.3.2.2.1 Terminal ID

The terminal identification will consist simply of the four (4) digit line number, which equates to four (4) characters.

4.3.2.2.2 Maximum Allowable Precedence

The maximum allowable precedence associated with a terminal specifies the highest precedence level with which that terminal can initiate a conference. The five precedence levels are FLASH OVERRIDE, FLASH, IMMEDIATE, PRIORITY, and ROUTINE. With each terminal ID, the maximum allowaole precedence can be specified in only one (1) character.

4.3.2.3 Satellite Configuration Table

This table will contain only the connector number to the CD port and the R/T number for the channel. Both of these data elements will require two (2) characters.

4.3.2.4 Authorized C^2 Terminals (at Other Node) Listing

Each conference director will have to keep updated in its memory a list of all authorized C^2 subscribers located at other SCP C^2 nodes who have the ability to utilize that node through AUTOVON/DSN connectivity in the occurence of network failures. It is recommended that these authorized C^2 users have at least the FLASH (or even the FLASH OVERRIDE) capability. It is also recommended that the number of terminals with this capability be small and that these terminals be located at CDs near the specified CD. The CD will require two (2) characters in memory to specify the secondary CD, four (4) characters to specify the associated terminal, and one (1) character to specify the maximum allowable precedence.

4.3.2.5 Pseudo Noise (PN) Code Table and KG Crypto Key Table

In order for the CDs to allocate satellite resources, they will have to acquire a PN code and KG key. Each table must have sufficient space to support status bytes for up to fifty (50) PN codes and status for up to fifty (50) KG keys. The required number of characters to specify these data elements are to be determined.

4.3.2.6 RED Switch Data Information Table

This table will contain all of the information required for the SCP to interoperate with the RED Switch network. Each RED Switch will either be collocated or directly connected via KG-84 encryption units to an SCP CD. Each SCP CD will contain the three digit code "NNX," signifying each RED Switch in the RS network. Associated with the code, each node will have to know which SCP CD is nearest the RED Switch. Therefore, establishing connectivity with a RED Switch over the SCP network will have to be done via the particular SCP CD nearest the desired RED Switch. The required data elements in the RED Switch Data Information Table resident in each conference director are as follows:

1. RED Switch Identification Code
2. Pointer to Collocated CD.

In addition, each CD will be required to maintain a listing of all C^2 STU-III users who can utilize the conference director. This will require a listing in memory of the terminal IDs and maximum allowable precedence.

4.3.3 Dynamic Data Tables

The Dynamic Data Tables will consist of data elements which will be constantly changing in relation to the status of the conference director at a particular time. The data elements in the dynamic data tables will change continually as defined by the needs of the system in performing the conferencing function. There will be two dynamic data tables associated with each conference director, as specified below:

1. Conference Information Table
2. Originator Status Table.

4.3.3.1 Conference Information Table

The Conference Information Table shall contain a listing of all the current on-going conferences in which the CD is the originator and/or the conferee. The contents of the Conference Information Table include the following data elements:

1. Conference ID
   - Node ID
   - Conference Control Number
2. Conference Status
3. Conference Type (Voice or Graphics)
4. Conference Precedence
5. Originators Phone Number
6. Pointers to Satellite Channels Assigned to the Conference
7. Pointers to status of KG keys and PN codes
8. Status of each of the Conferee Instruments in the Conference
9. Pointers to the Originator Status Table.

4.3.3.2 Originator Status Table

This table is used at the originator node of the conference only. This table shall contain the following information of all conferees not local to the node:

1. Conferee's Phone Number
2. Status of Conferees
   - Called
   - Ringing
   - Busy
   - Answered
   - On-Hook.

4.4 SCP C^2 CONFERENCING PROCEDURES

All SCP C^2 subscribers can originate and participate in SCP C^2 conferences. Preset and random SCP C^2 conference initiation will require data to be transfered among the different subsystems that comprise the SCP C^2 system. The primary vehicle to be used for transfering this information will be the Network Control Channel (NCC). The NCC shall be the means by which required information will be transfered in order to implement, maintain, and dissolve conferences. Conference control parameters will be transfered among the Network CDs via the NCC.

In SCP EOC [5], the NCC is a dedicated, full-period, Time Division Multiple Access (TDMA) channel. Each CD has access to a slot in the NCC TDMA ring in which to send the conference control parameters. However, it is not known whether the EOC NCC design will be used in SCP FOC. Therefore, this section will define 'he procedures and type of information which must be passed between the CDs to establish, alter, and terminate conferences; however, the specific NCC protocols that shall allow for the information transfer will not be given. In addition, since no information is available on the RED Digital Voice Terminal (RDVT) to be used in SCP FOC, the signaling modes and sequences required between a terminal and CD will not be given.

4.4.1 Entering C^2 Conference Data

The required data transfer and conference setup will be described for the establishment of preset and random conferences. If an originator exceeds his authorized capabilities, he will receive the appropriate announcement or tone (see Appendix C). Interoperation with the RED Switch network and GP as shown in Illustration 1-2 will also be discussed.

4.4.1.1 Preset Conference

The following description depicts the required information transfer and procedures involved in establishing a preset conference.

- User (originator) picks up handset
- User waits for dial tone
- User enters precedence, if conference precedence is not supplied, the CD shall assign the default precedence of ROUTINE
- User enters the preset conference selector code "#"
- User enters two digit preset conference number
- The CD checks the originators maximum allowable precedence to see if it allows him the precedence entered. If not, a tone is sent from the CD to the terminal.

4.4.1.2 Random Conference

The following description depicts the required information transfer and procedures which must be followed in establishing a random conference.

- User (originator) picks up handset
- User waits for dial tone
- User dials precedence of conference
- CD checks to see if the originator is within his maximum allowable precedence
- User dials access code and address of first conferee
- If the user has dialed the correct address, we recommend that he dial "*" to signify the completion of a correct address

- User dials each additional conferee in a similiar manner, again using "*" after a correct address
- If at any time the user dials an incorrect address, he may delete this address by dialing "#" as long as he has not signaled completion of a correct address
- After the last address has been signaled correct, the user dials "#" to signify the end of dialing.

4.4.1.3 SCP C^2 Bridging

This is the inherent or normal mode of SCP C^2 conferencing discussed in Paragraph 4.4.4.

4.4.2 STU-III Use of SCP C^2 CD

As previously mentioned, General Purpose STU-IIIs will not be authorized to originate SCP C^2 conferences. However, a few select C^2 users who do not have access to a RED Switch or SCP C^2 CD may utilize their STU-III to access the SCP C^2 CD. The method by which a C^2 STU-III user may access a SCP C^2 conference is nearly identical to a STU-III user originating a conference at the GP CD (Paragraph 3.4). The major difference is that C^2 STU-IIIs will be authorized to originate an SCP C^2 conference. These STU-IIIs can be identified in the following two ways:

1. Add an element in the STU-III ID Field indicating if the STU-III is authorized to originate SCP C^2 conferences

2. Have the SCP C^2. Keep a list of authorized C^2 STU-IIIs by storing the STU-III terminal ID in the data tables of the SCP C^2 CD. Since there are not that many remote C^2 users, we recommended that it be done this way. Once the STU-III is connected to the SCP C^2 CD, one can enter conferencing information the same as a directly connected SCP C^2 user does.

GP STU-III users are brought into an SCP C^2 conference in a similar manner as a STU-III is brought into a conference by a GP CD. The differences are that the STU-III must be cleared for TOP SECRET and the SCP C^2 CD will not bridge with any GP CD and will bring all STU-III (GP or C^2) conferees into the originator's CD through AUTOVON/DSN.

As mentioned before, the primary means of interconnecting C^2 users into a conference will be by the JRSC-allocated portion of the DSCS III satellite resources. For those conferences that will require a STU-III participant, the conference originator would have to dial the STU-III access code and address. His conference director would then access the desired STU-III user through AUTOVON/DSN resources. Before such a user can be brought into the conference, his STU-III will have to go secure with the C^2 RED Interface Terminal (RIT). Once the designated STU-III goes secure with the RIT, signaling regarding the connection must be sent from the RIT to the SCP CD. This information could, in turn, be passed on to the conference originator, if required. An example would be the passage of a busy signal or a tone to signify a successful call setup.

However, if the only way to bring a STU-III user into a conference is from the originator's conference node, the possibility of having to use terrestrial and transoceanic AUTOVON/DSN access lines could incur large delays and degraded voice quality. Take, for example, the following conference scenario: A C^2 node in Germany would like to setup a conference with NMCC and the ANMCC. The node also desires a GP conferee located at Ft. Ritchie, Maryland. As the conference originator, the C^2 call setup information would be passed over the Atlantic DSCS III satellite and the C^2 conference would be established according to SCP C^2 procedures. However, the GP conferee would have to be accessed by one of the AUTOVON/DSN access lines by the conference originator (Germany) dialing in the ten-digit identify of the GP user.

A possible alternative is having the C^2 conference director allow the conference originator to override the originator requirements and that once the C^2 connectivities are established, request the NMCC or ANMCC to bring in the Ft. Ritchie GP user. Therefore, the GP user could be brought into the conference not through a 5,000 mile AUTOVON/DSN access line, but through a considerably shorter AUTOVON/DSN access line. As mentioned previously, GP STU-IIIs will not be authorized to originate SCP C^2 conferences.

4.4.3 SCP C^2 To RED Switch

The planned SCP facilities, in many cases, will coexist with RED Switches. When SCP facilities and a RED Switch are collocated in a secure facility, direct RED analog trunk will be used to interconnect the RED Switch and the SCP CD. When a RED Switch and SCP CD are not collocated in a secure facility, the connections will be made by digitizing the RED traffic and sending it over a trunk with KG-84s at each end.

Due to different levels of security between the SCP C^2 CD and the RED Switch, and a lack of trusted software in the RED Switch, all conferences or calls between the two networks will only be self authenticating up to the SECRET security level. An announcement at the beginning of every conference or call stating this will be given whenever a RED Switch user is included. These calls may be verbally authenticated up to the TS/SCI level.

4.4.3.1 SCP C^2 User Accessing RED Switch Conference Bridge

When an SCP User or conference originator wants to conference with RED Switch subscribers, the SCP CD closest to the desired RS will have to be bridged with that RS analog conferencing bridge. The procedure for an SCP subscriber to initiate a conference involving RS subscribers is given below.

- User picks up the handset

- User waits for dial tone

- User dials the precedence

- The SCP CD checks to see if the originator's classmark allows him the precedence entered

- User will then dial the special feature code and the RS number for access to the RED Switch conference bridge

- If all lines from the SCP CD to the RS are presently in use at a higher precedence, then the SCP CD will give the subscriber a busy signal

- However, if any line is operating at a lower precedence, the SCP CD will preempt the line with the lowest precedence use standard MLPP procedures

- The SCP CD will then pass the precedence to the RED Switch through the use of tones

- If the number for the RS terminal is busy, the RED Switch will provide a busy signal, if there is no answer, the SCP CD will disconnect after 60 seconds

- Once a connection is established, the SCP subscriber will follow the same procedures for either a preset or random conference setup as given in Paragraph 5.4.

4.4.3.2 Adding a RS Subscriber to an Existing SCP C^2 Conference

If an SCP C^2 conference is already in progress, the originating C^2 user can add an RS subscriber as follows:

- The SCP conference originator will be required to hit the special "in conference" code "2" required for adding a subscriber(s)

- When the originating CD receives the dialed digit "2" from the conference originator, the originator is temporarily taken out of the conference in order to allow the originator to begin dialing precedence

- The originator will then hit the special feature code "80" for access to the RED Switch; following this he will dial the first RS number desired "NNX-XXXX"
- The originating CD will then send the desired terminal number over the NCC to the CD, which is collocated with the desired RS
- If all lines from the collocated SCP CD to the RS are presently in use at a higher precedence, then the SCP CD will give the subscriber a busy signal
- If, however, all lines are busy, but any one or more lines are operating at a lower precedence, the SCP CD will employ MLPP procedures
- Once the RS user is added to the conference, an announcement will inform all conferees that a SECRET user has joined the conference.

4.4.4 Conference Set-Up and Modification

The called terminal numbers will be placed in the NCC (according to the FOC NCC protocol structure) and transmitted via the NCC to the node controlling the called terminal. Upon receipt of the originating CD's message, the CD controlling the called terminal will reply over the NCC by sending the status of the called terminal. This status will be one of the following: "Busy," "Ringing," or "Answered." Once the originating CD receives word that one or more terminals are ringing, it will try to allocate an available voice/graphics satellite channel to the conference. If all channels are presently in use at higher precedence, then the CD will send an announcement to the originating terminal to signify this condition. However, if any other channels are operated at a lower precedence, MLPP will be employed. The satellite resources will be allocated to establish conference connectivity to the various satellite areas and conference nodes. If no called terminals are available to join the conference, then a tone will be sent from the CD to the originating terminal specifying this condition.

4.4.4.1 Conference Start

The conference will start when any one of the following conditions is met:

1. All conferees have answered and received an announcement that this is a conference call
2. After 60 seconds, all terminals that have not joined the conference will be determined unavailable and the conference will start. This time period is measured from the "end of dial" signal.

When the conference starts, the CD will make an announcement that the conference has begun.

4.4.4.2 Conference Modification

SCP conferencing requirements provide for such features as preemption, addition/deletion of conferees, and the ability to transfer the originator function to another conferee. This section will present the procedures for accomplishing the aforementioned requirements.

When an originator wishes to add a subscriber to an existing conference, he will dial the digit "2." When the originator CD receives the dialed digit "2" from the conference originator, the originator is temporarily taken out of the conference. The originator would then dial the conferee number.

For deleting a conferee from an existing conference, the originator will dial the digit "3." When the CD receives a dialed digit "3" while in the conferencing mode, it takes the conference originating terminal out of the conference temporarily. Then the originator will dial the conferee terminal number that is to be deleted. The CD collects the digits until the last digit of the conferee terminal is detected. The signal to terminate the conferee connection will be sent over the NCC. The CD with cognizance over the terminal will reply to the originator's NCC signal by issuing an announcement to the terminal to hang up. This CD will then update its conferencing and terminal status. The originating CD will then remove the terminal number and status information from its database and send an announcement stating that the action was accomplished to the originating terminal. Finally, the conference originator is placed back in the conference.

When an originator wants to transfer conference control to another user, he will dial the code number "8." When the CD receives the dialed digit "8" while in the conferencing mode, the originating CD will transfer conference originator control to the conferee identified by the terminal number entered by the conference originator. If the new originator is not attached to the same CD as the old originator, all of the conference information is sent over the NCC to the new originating CD.

The last requirements of the SCP system will be for the provision of conference and conferee preemption. When the CD at a node receives conference initiation information from the NCC and the new conference precedence is higher, the conference director shall send an announcement to the terminal stating "A higher precedence has preempted this conference." The subscriber should then hang up. Each of the user terminals taking part in the preempted conference will receive this announcement. If the terminal being preempted is the originator of an existing conference, all conference control information on the NCC having to do with the existing conference shall be deleted. At this point, the required satellite resources are reallocated for the use of the preemption conference.

4.4.4.3 Conference Termination

SCP C^2 conferences will not be terminated as long as one of the called parties and the conference originator are available. Once the conference originator hangs up or is preempted and has not transferred the originator's authority to anyone else, the conference will be terminated. Once this occurs, all terminals will receive a tone until they hang up.

SECTION 5 - RED SWITCH CONFERENCING

5.1 INTRODUCTION

The RED Switch subsystem supports C^2 secure voice users located within a physically securable enclave (RED enclave). Each RED Switch forms a switching hub for its own RED enclave. Users within the RED enclave will have 16 button Dual Tone Multifrequency (DTMF) telephone sets connected to the RED Switch by physically secured unencrypted loop circuits. RED switches will be networked together by direct encrypted RED Switch interswitch trunks. This allows users to exchange secure voice communication from low cost clear telephone sets. Some RED Switches will also have DSVT links to the TRI-TAC subsystems and trunks to collocated SCP CDs. RED Switches will also interoperate with STU-IIIs via RIT interfaces to AUTOVON/DSN telephone networks. These interoperation capabilities are shown in Illustration 1-2 and will be further discussed in Paragraph 5.4.

5.1.1 Assumptions

1. Only RED Switch users at the TOP SECRET security level may be authorized access to an SCP C^2 CD without authentication

2. Selection of the analog or optional digital conference bridge will be done automatically based on the trunk interface classmark

3. Many SCP C^2 CDs will be collocated with RED Switches

4. When RED Switches are bridged together, the switch serving as the secondary switch will not be allowed to bridge to another switch. In other words, tertiary bridging is not allowed

5. A single conferee is usually not brought in through a secondary switch; it is usually brought in directly

6. A RED Switch users classmark will not be transfered to an SCP C^2 CD

7. There will be no software security in the RED Switch

8. The RED Switch network will be SECRET high.

5.1.2 Operational Concept

The RED switch has an internal analog conference bridge or equivalent digital implementation that will provide preset and random conferencing when all members of the conference are RED switch subscribers. A RED digital conference bridge will be provided as an option. The RED switch is also capable of interoperating with external users and interconnecting with the SCP conference node. The RED switch provides trunk circuits for a variety of different equipment, including the STU-II and the STU-III.

The normal mode of operation in the RED Switch subsystem will be full duplex, but it will also support speaker/broadcast mode if necessary for interoperation. The RED Switch will be able to terminate and automatically interconnect intra-system lines to inter-system trunks employing Multilevel Precedence and Preemption (MLPP) call establishment procedures (see Appendix B). The RED Switch network will operate at system high SECRET with verbal authentication up to the TS/SCI level. This section will address the RED Switch Numbering Plan and Data Tables necessary for conference setup. Also interoperability with SCP C^2 and GP will be discussed.

5.2 NUMBERING PLAN

The numbering plan for the RED Switch network will be based on the Defense Switched Network (DSN) Worldwide Numbering Plan [1]. The numbering plan will permit calling within an interconnected network of RED Switches and include necessary features for interoperability with external networks and secure voice facilities. The numbers will be dialed on a RED telephone that will generate DTMF signals from a 4 x 4 dialing pad consisting of ten digits (0-9), the * and # symbols, and four precedence levels (FO, F, I, P). The following abbreviations will be used to designate the allowable range of digits in the numbering plan.

Designation	Digit Range
X	0-9
Y	0-1
N	2-9
K	2-7
A	8-9
P (Precedence)	(FO, F, I, P)

5.2.1 Precedence

The switching system will fully implement the Multilevel Precedence and Preemption (MLPP) scheme for all calls processed. The precedence digit, when required, will be the first dialed by the user. The precedence entry can be omitted for ROUTINE calls. The four levels of preemption are as follows:

FO	- FLASH OVERRIDE
F	- FLASH
I	- IMMEDIATE
P	- PRIORITY

This information will always be transfered to the desired address in order to initiate any necessary preemption.

5.2.2 Local Numbering

The local numbering plan will use a four digit line number for establishing intra-switch calls, to include calls to subordinate RSUs. Line number assignments will be in the form KXXX. Access to a local operator or host switch operator can be obtained by dialing zero "0".

5.2.3 Special Feature Codes

Codes for control of switch special features, such as conferencing, will be in the form *NX and #NX, where the * prefix will be used for initiation and the # prefix for cancellation. The * and # symbols can also be used in conference dialing, as discussed in conference setup. These codes will be changeable in the system software but should remain consistent with DSN-recommended assignments. For example, *26 corresponds to a random conference in the DSN.

5.2.4 Access Codes

Access to other networks and for inter-RED Switch calling will employ a two digit access code to designate the required network and type of service required.

Access code assignments will be of the form AX, and for system commonality the following access codes have been assigned.

Access Codes	Network/Service
80	Red Switch Network
81	Reserved
82	DSN/STU-II
83	DSN/STU-III
84	Tactical Network/DSVT
85	Spare
86	Reserved - SCP C^2
87	Reserved
88	AUTOSEVOCOM/KY-3
89	DSN/VTT
90	Local PABX/STU-II
91	Local PABX/STU-III
92	Commercial/STU-II
93	Commercial/STU-III
94-98	Spare
99	Reserved

5.2.5 Inter-RED Switch Dialing

Since RED Switches are interconnected in a network by digital trunks and trunk groups, the user dialing format for interswitch calls shall be of the form (P) - 80 - (NYX) - NNX - XXXX. The 80 represents the RED Switch network access code, NYX is the switch area code (omitted for intra-area calls), NNX or NNX-X is the switch office code, and the last four digits are the switch line address. Where a four digit office code is employed, the office code and line number overlap by one digit; therefore, the office code must be further constrained to the form NNX-K. The area and office codes for each switch will be the same as those assigned within the DSN for in-dial access to the RED Switch via its primary interface to DSN. So the final form for dialing internal to the RED Switch network is as follows:

(P) - 80 - (NYX) - NNX - KXXX

There are also standard directory line numbers for access to operator services from other RED Switches. These are assigned as follows:

Service	3 Digit Office	4 Digit Office
Operator Assistance	1110	N110
Chief Operator	1311	N311

5.3 RED SWITCH DATA TABLES

The electronic digital switching system inherent to the RED Switch will employ stored program control of redundant multitask microprocessors to perform call processing and other system features. The system software will be organized in a modular top-down structure with necessary data tables stored in routines and subroutines. In order to process random and preset conferences, the following data will have to be stored in a set of data tables.

5.3.1 RED Switch Data Elements

The RED Switch requires the following data to be present in order to establish a conference.

1. Originator ID (Line Number)
2. Originator's Authorization
   a. Maximum Allowable Precedence
   b. Access Code
   c. Maximum Calling Area
   d. Conferencing
      (1) Authorized random conference only

(2) Authorizea preset conference only

(3) Authorized preset and random

3. Preset Conference Data

a. List of Dialing Data

b. Identification of controlling station (authorized to delete charge list contents)

c. Numbers restricted to listen only

4. Conference Set-Up Data

5. Announcements and Tones (see Appendix C).

5.3.2 Data Element Description

When a user goes off-hook to originate a call or conference, the switch will access the data tables corresponding to that user. This classmark indicates each separate privilege, restriction, or special instruction for processing the user's calls. Classmarks can also be assigned to entire stations or groups of trunks if necessary.

5.3.2.1 Maximum Allowable Precedence

Each user in the RED Switch will be classmarked as one of five precedence levels:

FO	-	FLASH OVERRIDE
F	-	FLASH
I	-	IMMEDIATE
P	-	PRIORITY
R	-	ROUTINE

The switch will always check the user's dialed precedence to ensure it does not exceed his maximum allowable precedence.

5.3.2.2 Access Codes

If a user wants to dial outside of his local enclave, he must dial an access code for the desired network or service. Each user's classmark will define a list of access codes that he is authorized to dial. These access codes are listed in the numbering plan.

5.3.2.3 Maximum Calling Area (MCA)

Where user's access to the RED Switch or any other network is authorized, the user will be classmarked as one of five progressively wider MCA's for each network. Each MCA will be defined by both the DSN area codes and the switch codes permitted in each area code. The DSN area codes are broken into the following geographical areas: CONUS, Europe, Alaska, Caribbean, and Pacific. The switch codes could be anywhere from a few to all of the switch codes in the designated area. For example, the lowest calling area for a network shall be defined by up to twenty (20) authorized codes within a home area code.

5.3.2.4 Protocols

Conferencing internal to the RED Switch shall be provided on a full duplex basis unless the originator desires or requires the speaker/broadcast protocol. This can be stored in preset conference data or initiated by the user. Additionally, the conference will automatically be controlled to the speaker/broadcast protocol when connected to narrowband trunks that are appropriately classmarked.

5.3.2.5 Listen Only

Selected conferees shall be capable of being placed in a listen only or monitor mode. This designation will either be contained in the conference data of a preset conference or indicated by the user during random conference dialing.

5.3.2.6 Conference Authorization

Conferencing capability in the RED Switch network will be stored in the user's classmark. Users can be classmarked as follows:

1. Authorized random conference only
2. Authorized preset conference only
3. Authorized preset and random conferences.

The only restriction for being included in a conference is being restricted to listen only mode by the originator or preset conference information.

5.3.2.7 Preset Conference

User's classmarked to initiate preset conferences will do so by dialing the preset conference feature code, the conference precedence, and a two digit code of the desired conference. The two digit code is of the form XX, where X is any digit (0-9) defined in the numbering plan. This code will contain a list of numbers to be dialed by the switch, and these preset lists must also be capable of storing the following additional conference data:

1. Identification of the controlling station (authorized to delete/change list contents)
2. Identification of each conferee authorized to initiate the conference
3. Identification of each conferee restricted to listen only mode
4. Designation of speaker/broadcast protocol where desired.

If two or more preset codes are dialed, the switch will automatically eliminate duplicate conferee addresses. Reaching the attendant after the conference has begun could be handled similarly to special feature codes, and could only be done by the conference originator. An example would be dialing *0 or hitting the hookswitch. Appropriately classmarked station lines will be capable of providing hot-line (off-hook) initiation of a preset conference.

5.4 RED SWITCH CONFERENCING PROCEDURES

The normal mode of operation for conferencing will be full-duplex using the analog Conference Bridge (CB). The optional digital CB would automatically be used when two or more LPC-10 users are accessed through appropriately classmarked lines. The RS analog CB will be able to bridge with the SCP C^2 CD and the GP CD with restrictions as shown in Illustration 1-2.

5.4.1 Initial Connection to RED Switch

The following procedures should be followed before entering conference information:

- User picks up handset
- User (originator) waits for dial tone
- User dials special feature code for either random or preset conference
- The switch will check to see if the originator's classmark allows him to originate the desired type of conference
- User dials precedence
- The switch checks to see if the precedence is within the user's classmark
- The switch is now ready to receive conference data.

5.4.2 Entering Conference Data

Authorized originators will be able to initiate random and preset conferences. If at any time, the originator exceeds his authorized classmarking, the switch will return the appropriate announcement or tone.

5.4.2.1 Random Conference

Users authorized to initiate random conferences will do so as follows:

- User dials access code for the desired network of the first conferee
- The switch will check to see if the user's classmark permits him to access the desired network

- User dials full address of first conferee
- If the user has dialed a correct address, we recommend that he dial "*" to signify completion of a correct address. The user may then proceed with other conferees in a similar manner
- If the user dials an incorrect address, he may delete this address by dialing "#" as long as the completion of correct address had not been dialed for the present address
- The switch checks to see if the desired call is within the user's MCA
- After dialing "*" for the last complete correct address, the user dials "#" to signify end of dialing.

5.4.2.2 Preset Conference

Users authorized to initiate preset conferences would do so as follows:

- User dials two digit code for the desired preset conference
- User dials "*" after correct code or "#" to delete an incorrect code
- Switch checks to see if the user is authorized to originate the desired conference
- The user may then dial additional preset codes or random conferees using the same procedures shown above
- The switch will check to see if each additional conferee is in the user's MCA
- The user dials "*" after the last correct entry, then dials "#" to signify end of dialing.

5.4.2.3 RED Switch Bridging

Secondary conferences interval to the RED Switch network will be set up if the originator dials a preset conference where two or more conferees are located at a distant switch, or the originator sets up a random conference through the attendant with two or more conferees at a distant switch. When secondary conferencing is employed, the following process occurs:

- The primary switch accesses the secondary switch and indicates the need for a conference
- The primary switch transmits the dialing information to the secondary switch
- The secondary switch calls the conferees according to the dialing instructions sent by the primary switch
- The already established connection between the primary and secondary switch will be utilized to bridge the CBs together
- The secondary switch will store the numbers of unanswered or busy lines for possible retry and also transmit the numbers back to the primary switch for possible retry by the originator.

5.4.3 RED Switch To GP CD and STU-IIIs (GP and C^2)

For a RED Switch user to call the GP CD or a STU-III, he must be authorized access to the AUTOVON/DSN network.

5.4.3.1 Access to a STU-III

For authorized users to include a STU-III in a conference, the STU-III must be able to operate at least at the SECRET level. When the RED Switch user is dialing the STU-III, he must first dial the access code for the DSN network, then dial the DSN address. A single STU-III could be included in a RED Switch conference by the analog conference bridge. If more than one STU-III is included in the RS conference, the switch will automatically bring them in through the digital conference bridge to avoid voice degredation. Since there is presently no screening in the RED Switch, all RED Switch users will be classmarked the same in AUTOVON/DSN.

5.4.3.2 Accessing the GP CD

If, for some reason, a RED Switch user wishes to and is authorized to originate a conference at a GP CD, he may do so by either going through the RS attendant or dialing the CD directly through AUTOVON/DSN. If the RS user dials the CD directly, he must be able to control the secure dial mode on the RED Switch RIT. This could be done by dialing a code to enter or exit the secure dial mode at the RS/RIT. The RED Switch will appear as a single STU-III to the GP CD. Once connected to the GP CD, the RED Switch user would dial the conference information like any other STU-III (see Paragraph 3.4). There is, however, a problem with the classmark of the RED Switch user. How will the RED Switch user's classmarks be transfered to the RED Switch RIT? A few possible solutions are:

1. The RIT could be modified to accept this data from the RED Switch (modifications to the STU-III/RIT are discouraged)

2. The RITs attached to the RED Switch could be configured in several different sets of classmarks (this method is very unflexible and limits versatility in classmarking users)

3. All RITs from the RED Switch to GP could be supplied the same conferencing authority which would be that of the most limited authorized user.

4. All RITs from the RED Switch to AUTOVON/DSN could be supplied the highest conferencing authority, and the RED Switch would be modified to screen users based on line classmarking.

These are all possible solutions, but the most logical way to handle the problem would be to force the RED Switch user to set up the conference using the RED Switch conference bridge. Then it would be the conference bridge's responsibility to dial each STU-III directly.

5.4.3.3 RED Switch CB Bridging with a GP CD

Bridging of the RED Switch and a GP CD is planned to be a capability to authorized RED Switch users if the secondary conference is set up by the RED Switch attendant. However, this is not discussed in the RED Switch Performance Specification [2]. Therefore, a possible way of doing this is offered here.

For a RED Switch to bridge with a GP CD, the RED Switch must be able to emulate the functions of the primary GP CD discussed in Paragraph 3.4.2.3. The RED Switch attendant will be responsible for transfering data for a secondary conference at the GP CD. Therefore, the attendant must either be called first to set up the entire conference or be included as a conferee in a RED Switch conference.

When the conference originator has completed entering dialing data and the RED Switch attendant has determined that one or more GP CDs are required to set up the conference, the following occurs:

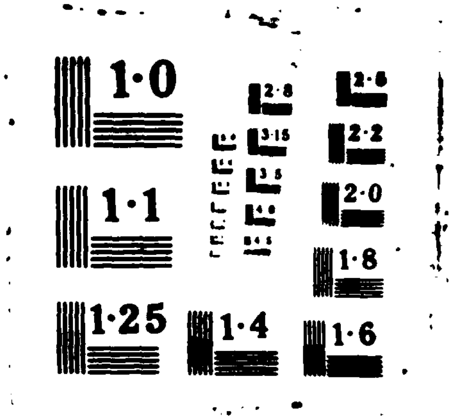
- The RED Switch attendant establishes a connection with the GP CD by calling the appropriate GP CD through an RIT and AUTOVON/DSN. If more than one GP CD is to be bridged, the RED Switch attendant will have to call each one individually

- AUTOVON/DSN connects the RED Switch/RIT to the GP RIT [illegible] using the standard MLPP procedures

- Once the two RITs have been connected, the RED Switch RIT transfers the following data to the GP CD RIT: terminal ID (containing RIT/CD ID), security [illegible] conference authorization, MCA (Note: conference authorization and MCA are sent but are [illegible] CBs are bridged; the RED Switch will [illegible] authorization and MCA of any [illegible]

AD-A177 932 SECURE VOICE SYSTEM INTEGRATED CONFERENCING ANALYSIS 2/2
AND INTEROPERATION DESIGN(U) COMPUTER SCIENCES CORP
FALLS CHURCH VA SYSTEMS DIV G KNOWLES ET AL. 17 FEB 87
UNCLASSIFIED DCA100-84-C-0030 F/G 17/2 NL

END
4 87
DTIC



1·0
2·8
2·5
3·15
2·2
3·5
2·0
1·1
4·0
1·8
1·25
1·4
1·6

- When the RIT of the RED Switch and the RIT of the GP CD synchronize, the RED Switch instructs its RIT to go into the secure dialing mode
- The RED Switch attendant sends the GP CD a code indicating that a RED Switch wishes to establish a secondary GP conference
- The RED Switch attendant transmits the dialing information to the GP CD
- The GP CD calls the conferees according to the dialing instructions sent by the RED Switch attendant
- The already-established connection between the RED Switch and GP CD will be utilized to bridge the CBs together (the RED Switch CB will automatically revert to the speaker/broadcast mode when bridged with a GP CD).

5.4.4 RED Switch to SCP C^2 CD

Authorized RED Switch users will be able to conference with SCP C^2 users by bridging the SCP C^2 CD to the RED Switch analog CB. When the SCP CD and the RS are collocated in a secure facility, a direct RED analog trunk will be used to connect the RS and the SCP CD. When they are not collocated in a secure facility, the connection will be made by digitizing the RED traffic and sending it over a trunk with KG-84 encryption devices at each end. The speaker/broadcast protocol will automatically be used when conferencing between the RS and SCP.

There are a few problems that must be resolved inorder for RED Switch user and originate an SCP C^2 conference. The first problem is that of security. The RED Switch is SECRET high but the SCP C^2 is TOP SECRET high. Also, there is no trusted software security in the RED Switch, therefore, this will require all connections between the RED Switch and SCP C^2 CD to be originated at the SECRET level and verbally authenticated up to the TS/SCI level when necessary. Since the SCP C^2 CD is system high TOP SECRET, an announcement must be made at the beginning of each conference with RED Switch users or whenever a RED Switch user is added to an existing conference to inform all SCP C^2 users that the conference is presently at the SECRET level.

Another problem could be transfering the maximum allowable precedence of the conference, since the SCP CD does not know the classmark of the originator in the RS. Since the SCP CD would not be able to recognize the terminal number when someone behind the RS is calling the SCP CD, it is not known how the classmark indicating the maximum allowable precedence for an originator behind the RED Switch can be transferred from the RED Switch to the SCP CD. This could be done in one of the following ways:

1. This alternative would allow interoperation from the RS to the SCP CD without requiring the maximum allowable precedence associated with an RS terminal to be passed to the SCP CD. This could be done by classmarking different lines corresponding to the different precedence levels; thus, when the RED Switch verifies that the terminals maximum allowable precedence allows it to make a call to the RS at the precedence chosen by the originator, the RS would place the call through on a line corresponding to the precedence level chosen by the originator terminal. Both the RS and SCP CD would have to keep a list of all lines between them in their data tables with the corresponding precedence levels on those lines that would signify the precedence of the conference. This alternative has a serious disadvantage regarding the allowance of preemption between the RS and SCP CD.

2. This alternative would entail establishing a signaling channel between the RED Switch and SCP CD so conference control information could flow between both elements.

This channel would be used to provide conference status between these elements and to assist in the conference setup process. The problem with this alternative is that a capability for a signaling channel is not mentioned in either SCP or RED Switch documentation.

3. The RED Switch will receive as the first digit dialed from the conferee terminal the precedence. After verifying the precedence with the originator's classmark, the RS could transfer the required precedence to the SCP CD through the use of five different tones to signify the five different precedence levels.

It is recommended that Alternative #3 be chosen as the preferred method for allowing interoperation between the RS and SCP CD elements and will be used for describing the conference setup for the RS and SCP C^2 CD.

5.4.4.1 Accessing the SCP C^2 CD

The following is list a of procedures for establishing a conference or call from a RED Switch subscriber to the SCP CD:

- RS user (originator) picks up handset
- User waits for dial tone
- User dials the precedence
- RS checks to see if the originator's classmark allows him the precedence entered
- User then dials the special feature code for the SCP CD (which is directly connected to the RS)
- RED Switch will check to see if the user's classmark allows him to call into SCP
- If all lines going into the SCP CD are presently in use at higher precedence, then the RED Switch will give the user a busy signal

- If all lines are presently busy, but if any lines are operating at a lower precedence, the RED Switch employ MLPP precedures
- The switch will then send a tone to the SCP CD indicating the precedence of the call
- At this time, the RS subscriber to the SCP CD appears like any SCP subscriber and the RS subscriber will initiate the call or conference (whether preset or random) by the SCP dialing procedures given in Paragraph 4.4
- The RS originator may hit a hook switch, or some other form of signaling that will not be propagated to the SCP CD, to return to normal RED Switch conference dialing mode.

When subscribers within the RS are already conferencing, the RED Switch analog conferencing bridge can bridge with the SCP CD when adding SCP subscribers. In this situation, the RS will act as the primary conferencing bridge and the *SCP CD as the secondary* conferencing bridge.

5.4.4.2 RED Switch and SCP C^2 Bridging

Bridging the SCP conference director and RED Switch analog conferencing bridge will be done with either the SCP CD or the RS CB acting as the primary conferencing bridge, depending on whether the originator is an RS subscriber or an SCP subscriber. Although it is not discussed in any of the Performance Specifications [2][7], it is recommended that information be transferred between the bridges in the following manner:

- The primary bridge will send the secondary bridge a secondary conference feature code
- The primary bridge will transmit the dialing information to the secondary bridge

- The secondary bridge calls the conferees according to the dialing instructions sent by the primary bridge

- The secondary bridge will send back to the primary bridge the status of each terminal by the use of either "Ringing," "Busy," or "Answered" code words

- For conferencing between the bridged conferencing bridges, the speaker/broadcast protocol shall be utilized

- Any specialized announcements or tones during the conference should be sent from the primary conferencing bridge.

5.4.5 Conference SetUp and Modification

When the user signals end of dialing, the switch checks to see if there are sufficient idle ports to complete the desired call. If necessary, the switch will employ MLPP precedures to gain access to the necessary ports. If there is still an insufficient number of ports available, the switch will return a busy signal to a ROUTINE originator and a "Blocked Precedence" announcement to a higher precedence originator. Once the switch gains the sufficient number of ports, it initiates connections to each conferee. If more than one conferee is located at the same distant RED switch, the primary switch will dial the secondary switch and bridge the two together if this conference was preset or setup through the attendant.

5.4.5.1 Conference Start

The conference will start when one of the following conditions is met:

1. After 10 ROUTINE precedence ring cycles (60 seconds), all busy or unanswered terminals will be disconnected, but the numbers will temporarily be stored for possible retry by the originator. At this point the conference will begin

2. The conference will begin once all conferees have answered and received the announcement that this is a conference call.

5.4.5.2 Conference Modification

A RED Switch conference originator must be able to add conferees to an ongoing conference and transfer the originators status during a conference. This will be done by dialing a code for the action desired and dialing the address of the conferee. It may also be done by accessing the RS attendant in a similiar manner and letting the attendant perform the desired operation. It might be helpful to use the same codes that the SCP C^2 CD uses to improve compatibility and system commonality. The originator may only transfer the originating status to a conferee at his same switch.

5.4.5.3 Conference Termination

Conferences will be maintained as long as one local station and any other conferee remain connected. Conferees going on-hook will result in a distinct tone transmitted to all other conferees. If a primary conference is preempted, any secondary conference may continue, but only at the ROUTINE level.

APPENDIX A - STU-III FAMILY

A.1. INTRODUCTION

The Future Secure Voice System (FSVS) project is a major initiative to develop and deploy a new generation of secure telephone equipment. This undertaking is being sponsored by the National Security Agency (NSA) and combines NSA's knowledge of cryptography with the experience and capabilities of the telecommunications industry for design and production of the STU-III.

The STU-III will replace the STU-II (KY-71) and AUTOSEVOCOM terminals as the principal terminal of the Secure Voice System. The STU-II was designed for a projected use of less than 10,000 users. However, analysis of government and related user requirements has put the number of users requiring a secure voice capability as high as a million. The STU-III has been designed to satisfy this high population requirement by meeting such objectives as a manageable keying scheme, low unit price, and user-friendliness.

A.2 DESCRIPTION

The FSVS program philosophy is to provide the secure voice capability to the DoD, military C^2, general purpose users, civil agencies, defense contractors, and the private sector. There are three separate versions of STU-III terminals in the FSVS. The STU-III Type I Low Cost Terminal (LCT) is for use by the government and government contractors to protect information of a classified or sensitive nature. The STU-III Type II LCT is for use by any government agency, corporation, or individual to protect unclassified information (including national security-related information). The C^2 STU-III (the KY-77 is presently being redirected), is a Type I terminal that provides a number of special performance features required to support Command and Control and Mobile applications. The C^2 STU-III will be able to directly interoperate with the STU-II and STU-III Types I and II terminals. A comparison chart between the C^2 STU-III (KY-77) and the STU-III Type I LCT is shown in Illustration A-1.

The STU-III Type II LCT will not be able to process classified voice; therefore, it will not be utilized by SVS users for secure voice conferencing. Because of this fact, all discussion concerning STU-III operation in this document will henceforth refer to STU-III Type I LCT operation only.

A.3 KEYING CONCEPT AND MANAGEMENT

The FSVS will use a keying concept termed Firefly II. Firefly II is an enhanced version of the public key algorithm that allows two terminals to generate their own per-call key, which is a random sequence of bits that are exchanged with one another in order to set up a secure connection. This concept is based upon the application of three types of key protection; Key Encryption Keys (KEKs), Traffic Keys (TKs), and Crypto Ignition Keys (CIKs). KEKs are used during the secure call set up or during electronic rekey. TKs are used between two STU-IIIs on a per-call basis. CIKs are used by the users to lock and unlock terminals for use in the secure mode.

For each secure call, the two STU-IIIs use a different Traffic Key to encrypt the voice or data throughout the duration of the call. Both terminals cooperate in establishing the Traffic Key by each terminal generating a portion of the Traffic Key. This key set up requires no interaction with a Key Distribution Center, as did the STU-II BELLFIELD Key Distribution system. Distribution of the two portions of the Traffic Key is via signaling protected in the Key Encryption Keys of the terminal. Therefore, each STU-III requires a unique "custom" KEK.

The unique "custom" key can be loaded into a terminal in two different ways. The first is by way of a seed key. This entails ordering a Fill Device (FD), which contains the seed key

Feature	TYPE I LCT	KY-77(*)
Clear/Secure Operation	X	X
2.4 KBPS (LPC-10) Voice	X	X
2.4 KBPS Data	X	X
4.8 KBPS Voice	Option	
Per-call Electronic Keying	X	X
MLPP (Four-wire)	Option	X
HEMP	Option	X
Net Mode Operation		X
MILSPEC		X
MLPP (Two-wire)	Option	Option
Multi-line (Bell IA2)	Option	Option
STU-II Interoperability	Manual Gateway	X
ANDVT Interoperability	Interface to be developed	X

* The KY-77 program is presently being redirected.

Illustration A-1. STU-III Type I LCT/KY-77 Features Comparison information from the Key Management Ordering and Distribution Center (KMODC). This FD is an unclassified piece of hardware. The key is then physically loaded from the FD during installation. When the FD is inserted into the terminal, the key will be read from the FD into the terminal. Once loaded, the seed key can be used only once to secure a call between the STU-III and the Key Management Center (KMC). The KMC electronically distributes an operational key to the STU-III terminal. Once the STU-III has an operational key, it can set up a secure call to any other STU-III without any interaction with the Key Management System. A call to the KMC only needs to be made once for initiation of the STU-III terminal and then only once a year for rekeying.

The other way to load the unique "custom" key is to order a classified fill device (FD) from the KMODC, which includes the operational key on it. Once again, when the FD is loaded into the terminal, the key will be read from the FD into the terminal. The terminal then reads the key, checks it, and transfers keying information into its memory. This time, however, no call to the KMC is required, since the "custom" key information was on the FD and extracted by the terminal. The operational key is classified to the highest classification level of traffic that has been approved and authorized for the terminal. The only basic difference between the initiation involving a seed key versus an operational key is that with an operational key a call is not required to the KMC during initiation.

The terminal knows whether the operational or seed keying information reside on the FD by reason of different ID Field information. Once the FD has been zeroized during the initiation process, that device now becomes a Crypto Ignition Key (CIK). This is the key for everyday use which, when inserted, will allow secure mode operation. Removing the CIK from the terminal disables secure communications; however, normal (non-secure) telephone communications are still provided. After the fill device becomes the first CIK, up to a total of seven more CIKs may be made during the initiation process.

After the initial loading of the key, the terminal will need to be rekeyed only once yearly. For a rekey, the user will dial an 800 commercial number that connects him with the KMC. The KMC will answer the call and place the terminal in the secure mode. The rekey will be sent electronically over the network. The KMC will then terminate the call. This entire process lasts only one minute. The key management system is shown in Illustration A-2.

A.4 STU-III FEATURES AND CAPABILITIES

The STU-III design incorporates many features and capabilities. One of the most important security features is the authentication process required in the secure call set up between two terminals. This data will include both a user identification (e.g., by division, department, or, more specifically, the user name) and the highest clearance level of that user/terminal. The STU-III terminal display will project the highest clearance level common to both users, thus allowing the conversation to exist up to that level.

The STU-III has other security features. Simply by removing the Crypto Ignition Key (CIK) from the terminal, the STU-III is unclassified and no after-hour controls are needed. Additionally, if a compromise of a STU-III terminal or key has occurred, a process exists that will disallow other STU-IIIs from going into the secure mode if called by the compromised terminal. Compromised terminal IDs will be placed into a STU-III's ID Field information either upon a call to the KMC or once another terminal has this information. This is a self-propagating procedure of disseminating this information to the community of STU-III users. Each STU-III should be capable of storing 500 such compromised terminal IDs in memory.

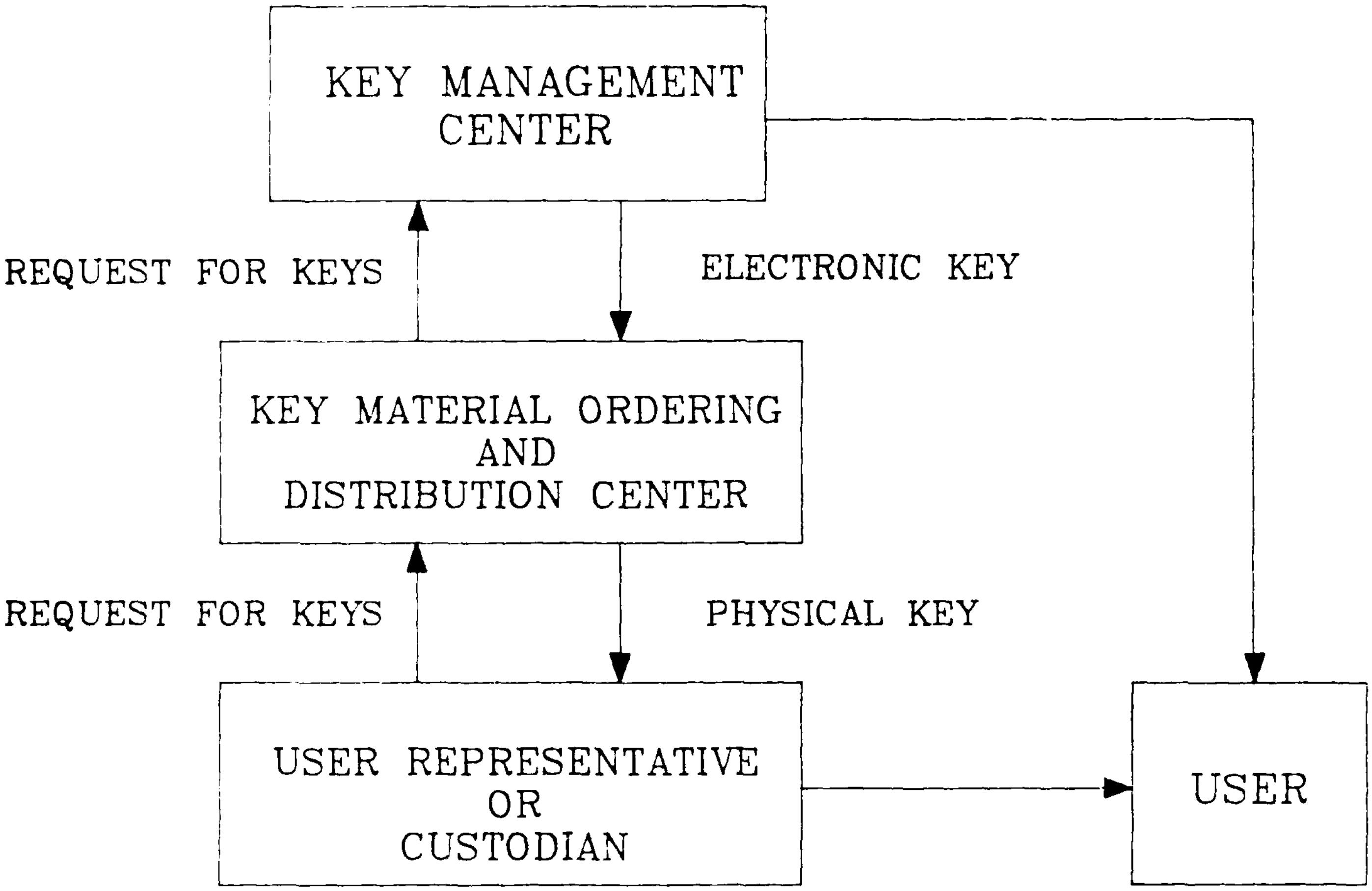


Illustration A-2. Key Management Overview

The STU-III vendors must meet a set of minimum essential requirements (MERs). However, they are able to add additional features. All STU-III terminals will interoperate in two modes. These modes are the 2400 bps secure voice mode and the 2400 bits-per-second secure synchronous data mode. The terminals will use the LPC-10 enhanced voice digitizing algorithm, which is compatible with the government standard LPC-10. The vendors are free to allow other data rate modes on their designed STU-IIIs; however, for interoperability with all STU-IIIs they will have to automatically adapt to the 2.4 kbps data rate.

Some of the common features inherent in all FSVS terminals are given below:

- Both pulse and DTMF loop signaling to allow STU-III compatibility with planned and existing networks, including AUTOVON/DSN
- A multi-level precedence/preemption option for interoperation over AUTOVON/DSN precedence signaling
- An RS-449 synchronous data interface at 2400 bps
- Two-line alphanumeric display to provide the user with instructions, the security classification level authorized for a call, and the ID number of the distant terminal
- A standard "Fill Device" to physically load key into the terminal.

Since the STU-III has been designed in a modular fashion, future enhancements and special requested requirements will be possible. Some examples are the inclusion of a push-to-talk capability, and a 4 x 4 keypad for AUTOVON/DSN precedence dialing.

APPENDIX B - MULTILEVEL PRECEDENCE AND PREEMPTION (MLPP) FOR CONFERENCES

The three major subsystems (GP, SCP C^2, RED Switch) of the SVS System will be designed in such a manner as to fully implement the National Communications System Voice Precedence System for a teleconferencing and telecommunications services provided. This precedence system, referred to as Multilevel Precedence and Preemption (MLPP) provides for five (5) levels of precedence and four levels of preemption. The rank order of precedence being:

FLASH OVERRIDE	(FO)
FLASH	(F)
IMMEDIATE	(I)
PRIORITY	(P)
ROUTINE	(R)

Each user in the SVS will be classmarked with one of the five precedence levels alone and will be restricted from initiating a conference above that level. The precedence of each conference will be determined as part of the dialed address.

Upon completion of dialing, the necessary idle ports, if available, will be seized and the conference connections attempted. If all conference bridges are busy, ROUTINE conference call attempts shall receive a "Line Busy" tone and conference call attempts above ROUTINE will re-examine all conference bridges on a preemptive basis. The selection of a conference for preemption will be based on the following:

1. Select the lowest precedence conference below the dialed precedence with sufficient ports.
2. If one conference is not enough, select the smallest number of equal precedence conferences below the dialed precedence with sufficient ports.

3. Select the smallest number of conferences below the dialed precedence required to provide sufficient ports.

When a conference is preempted, a three second burst of preempt tone will be provided to all connected lines and trunks prior to releasing the conference connections. When a single conferee is preempted, the conferee will receive the preempt tone while the rest of the conferee will receive a normal conferee release tone. Preempted bridges will automatically send an on-hook signal to the associated switch ports to permit new connections. Where the requested precedence is equal to, or lower than, that of the necessary number of ports to complete a conference call, the originator will be provided a "Blocked Precedence" announcement.

APPENDIX C - ANNOUNCEMENTS AND TONES IN THE SVS

Announcements and Tones will be distributed throughout the SVS. They will be stored in conference directors, switches, and even AUTOVON/DSN. These announcement tones may apply to incoming or outgoing calls. Different subsystems may require more announcements or tones, but for interoperation all users should be able to recognize at least the following list of announcements and tones:

Blocked Precedence "Equal or higher precedence calls have prevented completion of your call. Please hang up and try again. This is a recording."

Unauthorized Precedence "The precedence used is not authorized for your line. Please use an authorized precedence or ask your operator for assistance. This is a recording."

Precedence Access Limitation "Precedence access limitation has prevented the completion of your call. Please hang up and try again. This is a recording."

Unassigned "Your call cannot be completed as dialed. Please consult your directory and call again; or ask your operator for assistance. This is a recording."

Reorder "Your call has not been completed. Please hang up, and call again. This is a recording."

Station Disabled "The number you have dialed has been temporarily disabled. Please call again at a later time; or hold for operator assistance. This is a recording."

Unauthorized Calling Area "The number you have dialed is not authorized on your line. Please consult your directory; or ask your operator for assistance. This is a recording."

Service Interruption "A service disruption has prevented the completion of your call. Please wait 30 minutes and try again. In case of emergency, call your operator. This is a recording."

Conference Participation "Please stand by to participate in a conference call."

Conference Monitor "Please stand by to monitor a conference call."

Conference Initiation "The conference will now begin."

Secure Dial Prompting "Please enter the secure dial mode and dial the desired (switch location or organization) extension number."

Operator Queue Notification "All operators are busy on equal or higher precedence calls. Please hold and your call will be placed in queue. This is a recording."

Queue Preempt Notification "Your call has been preempted from queue due to high precedence traffic. Please hang up and call again. This is a recording."

Signal	Frequencies (Hz)	Frequency	Composite Level	Interruption Rate	Tone On	Tone Off
Dial Tone	350 + 440 (Mixed)	-13 dBm0	-10 dBm0	Continuous	---	---
ine Busy Tone	480 + 620 (Mixed)	-24 dBm0	-21 dBm0	60 IPM	0.5 sec	0.5 sec
Reorder Tone	480 + 620 (Mixed)	-24 dBm0	-21 dBm0	120 IPM	0.2 sec	0.3 sec
o Circuit (Trunk Busy Tone)	480 + 620 (Mixed)	-24 dBm0	-21 dBm0	120 IPM	0.2 sec	0.3 sec
udible Ringing (ROUTINE Call)	440 + 480 (Mixed)	-16 dBm0	-13 dBm0	10 IPM	2.0 sec	4.0 sec
Audible Ringing (Precedence Call)	440 + 480 (Mixed)	-16 dBm0	-13 dBm0	30 IPM	1.64 sec	0.36 sec
reemption Tone	440 + 620 (Mixed)	-18 dBm0	-15 dBm0	Continuous	---	---
ermanent Tone	350 + 480 (Mixed or Howler Type)	-17 dBm0	-14 dBm0	Continuous	---	---
Conference isconnect Tone	852 and 1336 (Alternated at 100 ms. Intervals)	-24 dBm0	-21 dBm0	Continuous	2.0 sec (per occurence)	---

llustration C-1. Information Tones for the SVS

REFERENCES

[1] "Defense Switched Network Generic Switching Center Requirements," DCEC-R610-001, Defense Communications Engineering Center, 15 October 1985.

[2] "Draft Engineering Performance Specification For A RED Telephone Switching System." Defense Communications Engineering Center, October 1985.

[3] "Installation and Implementation Plan For Phase I of the Secure Conference Project in the PACOM (CONFIDENTIAL)," Naval Electronic Systems Command, 10 October 1984.

[4] "JRSC System Engineering Performance Analysis (SECRET)," Defense Communications Engineering Center, June 1986.

[5] "Secure Conference Project Early Operational Capability Functional Description (CONFIDENTIAL)," Naval Ocean Systems Command, 11 February 1983.

[6] "Secure Voice System Goal Architecture," 4 February 1986.

[7] "System Specification (TYPE A) For The Secure Conference Project," DCEC R630-003, Denfense Communications Agency, 1 October 1984.

GLOSSARY

ADM-DCD	Advanced Development Model Digital Conference
ANDVT	Advanced Narrowband Digital Voice Terminal
ANMCC	Alternate National Military Command Center
AUTOSEVOCOM	Automatic Secure Voice Communications
AUTOVON	Automatic Voice Network
bps	Bits Per Second
CB	Conference Bridge
C^2	Command and Control
CD	Conference Director
CIK	Crypto Ignition Key
CINC	Commander in Chief
COMSEC	Communication Security
CONUS	Continental United States
CSC	Computer Sciences Corporation
DCA	Defense Communications Agency
DCAOC	Defense Communications Agency Operations Center
DoD	Department of Defense
DSCS	Defense Satellite Communications System
DSN	Defense Switched Network
DSVT	Digital Subscriber Voice Terminal
DTMF	Dual Tone Multifrequency
ECCM	Electronic Counter-Countermeasures
ELANT	East Atlantic
EOC	Early Operational Capability
EPAC	East Pacific
ETS	European Telephone System
FD	Fill Device
FOC	Final Operational Capability
FSVS	Future Secure Voice System
GP	General Purpose
HEMP	High Altitude Electromagnetic Pulse
ID	Identification
IO	Indian Ocean
JCS	Joint Chiefs of Staff
JRSC	Jam Resistant Secure Communications
KDC	Key Distribution Center
KEK	Key Encryption Keys
KG-81	Trunk Group Encryption Device
KG-84	Trunk Encryption Device

KMC	Key Management Center
KMDDC	Key Management Ordering and Distribution Center
KY-77	Command Control Version of STU-III
LCT	Low Cost Terminal
LPC	Linear Predictive Coding
MCA	Maximum Calling Area
MILSPEC	Military Specification
MLPP	Mulitlevel Precedence and Preemption
MRVT	Multiple Rate Voice Terminal
NCA	National Command Authorities
NCC	Network Control Authorities
NEACP	National Emergency Airborne Command Post
NMCC	National Military Command Center
NSA	National Security Agency
OSD	Office of Secretary of Defense
PABX	Private Automatic Branch Exchange
PACOM	Pacific Command
PBX	Private Branch Exchange
PN	Pseudo Noise
RDVT	RED Digital Voice Terminal
RED	Unencrypted
RED Switch	PBX Certified to Process Calssified Voice Traffic
RIT	RED Interface Terminal
RS	RED Switch
R/T	Receive/Transmit
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCP	Secure Conference Project
STU-II	Secure Telephone Unit (Second Generation)
STU-III	Secure Telephone Unit (Third Generation)
SVI	Secure Voice Instrument
SVS	Secure Voice System
TDMA	Time Division Multiple Access
TK	Traffic Key
TRI-TAC	Tri-Service Tactical Communications
TRS	Telecommunications Service Request
TS	Top Secret
UTS	User Terminal Subsystem
WLANT	West Atlantic
WPAC	West Pacific